NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE COMBINED ENTERPRISE REGIONAL INFORMATION EXCHANGE SYSTEM – THE WAY AHEAD

by

Douglas A. Cook
Patrick E. Lancaster Jr.
Robert R. Patto Jr.

September 2007

Thesis Advisor:	Karl Pfeiffer
Co-Advisor:	Buddy Barreto

Approved for public release; distribution unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE The Combined Enterprise Regional Information Exchange System – The Way Ahead	**5. FUNDING NUMBERS**
6. AUTHOR(S) Douglas A. Cook, Patrick E. Lancaster, Jr., Robert R. Patto, Jr.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The Combined Enterprise Regional Information Exchange System (CENTRIXS) is a coordinated Department of Defense Program established at the request of the Combatant Commands (COCOMs) to support the Global War on Terrorism (GWOT). CENTRIXS is a standing, global enterprise network allowing U.S. and coalition nations and their forces, in a seamless manner, to securely share operational and intelligence information in support of combined planning, a unity of effort, and decision making in multinational operations.

This thesis describes CENTRIXS networks that support the needs of the COCOMs on a global basis. The document also addresses who is connected to whom, what kinds of information must be passed from one user to another, and the services provided to the users of CENTRIXS networks. We conduct a Knowledge Value Added analysis to streamline the manning and usability of CENTRIXS nodes. We also explore how to efficiently and effectively go through the process of acquisition, installation, and accreditation of a CENTRIXS node.

14. SUBJECT TERMS Defining CENTRIXS, Increasing the Value of CENTRIXS, Acquisition, Installation, and Accreditation	**15. NUMBER OF PAGES** 155
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

THE COMBINED ENTERPRISE REGIONAL INFORMATION EXCHANGE SYSTEM – THE WAY AHEAD

Douglas A. Cook
Captain, United States Marine Corps
B.A., North Carolina State University, 1998

Patrick E. Lancaster, Jr.
Lieutenant, United States Navy
B.S., Southern Illinois University, 1997

Robert R. Patto, Jr.
Lieutenant, United States Navy
B.S., The College of William & Mary, 1998

Submitted in partial fulfillment of the
Requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2007

Authors: Douglas A. Cook

Patrick E. Lancaster, Jr.

Robert R. Patto, Jr.

Approved by: LtCol Karl Pfeiffer
Thesis Advisor

Albert (Buddy) Barreto
Co-Advisor

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Combined Enterprise Regional Information Exchange System (CENTRIXS) is a coordinated Department of Defense Program established at the request of the Combatant Commands (COCOMs) to support the Global War on Terrorism (GWOT). CENTRIXS is a standing, global enterprise network allowing U.S. and coalition nations and their forces, in a seamless manner, to securely share operational and intelligence information in support of combined planning, unity of effort, and decision making in multinational operations.

This thesis describes CENTRIXS networks that support the needs of the COCOMs on a global basis. The document also addresses who is connected to whom, what kinds of information must be passed from one user to another, and the services provided to the users of CENTRIXS networks. We conduct a Knowledge Value Added analysis to streamline the manning and usability of CENTRIXS nodes. We also explore how to efficiently and effectively go through the process of acquisition, installation, and accreditation of a CENTRIXS node.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS AND ACRONYMS

AAP	Accelerated Acquisition Plan
ACAT	Acquisition Category
ADNS	Automated Digital Network System
ALT	Actual Learning Time
AOR	Area of Responsibility
ARID	Active Reviews for Intermediate Design
AS	Acquisition Strategy
ASD	Assistant Secretary of Defense
ATAM	Architecture Tradeoff Analysis Method
BDA	Battle Damage Assessment
BSC	Backup Domain controller
C2	Command and Control
C2PC	Command and Control Personal Computer
C4I	Command, Control, Communications, Computers, and Intelligence
CANES	Consolidated Afloat Network and Enterprise Services
CAS	Collaboration At Sea
CCA	Clinger-Cohen Act
CCC	Coalition Coordination Cell
CCEB	Combined Communications Electronics Board
CCIB	Command and Control Interoperability Board
CDD	Capability Development Document
CDI	Cooperative Defense Initiative
CDS	Cross Domain Solutions
CENTRIXS	Combined Enterprise Regional Information Exchange System
CFBLNet	Combined Federated Battle Laboratory Network
CFE	CENTRIXS Four Eyes
CIO	Chief Information Officer
CIP	Common Intelligence Picture
CIS	Coalition Information Sharing
CJCS	Chairman of the Joint Chiefs of Staff
CJTF	Combined Joint Task Force
CM	Configuration Management
CMM	Capability Maturity Model
CNCC	CENTRIXS Network Control Center
CND	Computer Network Defense
CNO	Computer Network Operations
COCOM	Combatant Commander
COI	Community of Interest
COMPOSE	Common PC Operating System Environment
COP	Common Operational Picture

COTS	Commercial Off The Shelf
COWAN	Coalition Wide Area Network
CPD	Capability Production Document
CPMO	CENTRIXS Program Management Office
CPOK	CENTRIXS Portable Operation Kit
CRD	Capstone Requirements Document
CSFL	Common Systems Function List
DAA	Designated Approving Authority
DAO	Defense Attaché Office
DAS	Defense Acquisition System
DATT	Defense Attaché
DERF	Defense Emergency Response Fund
DIA	Defense Intelligence Agency
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISR	Defense Information Systems Registry
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
DOTMLPF	Doctrine, Organization, Training, Material (Technology), Leadership and Education, Personnel (Culture) and Facilities
DoD	Department of Defense
DRR	Design Readiness Review
DS	Decision Support
DSS	Decision Support System
DUSD(I)	Deputy Under Secretary of Defense for Intelligence
EA	Executive Agent
EIE	Enterprise Information Environment
ET	Electrical Technicians
FAA	Functional Area Analysis
FAK	Fly Away Kit
FCB	Functional Capability Board
FDO	Foreign Disclosure Officer
FIT	Fleet Installation Training
FL	Force Level
FNA	Functional Needs Analysis
FOC	Full Operational Capability
FoS	Family of Systems
FSA	Functional Solution Analysis

GAL	Global Address List
GCC	Gulf Cooperation Council
GCCS	Global Command and Control System
GCTF	Global Counter Terrorism Force
GIG	Global Information Grid
GOTS	Government Off The Shelf
GWOT	Global War on Terrorism
IA	Information Assurance
IADT&L	Integrated Defense Acquisition, Technology and Logistics
IAVA	Information Assurance Vulnerability Alerts
ICD	Initial Capability Document
IERs	Information Exchange Requirements
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
INFOSEC	Information Security
IO	Information Operations
IOC	Initial Operational Capability
IPL	Integrated Priority Lists
ISEA	In Service Engineering Activity
ISNS	Integrated Shipboard Network System
ISO	International Standards Organization
ISP	Information Support Plan
ISR	Intelligence, Surveillance and Reconnaissance
ISSE	Information System Security Engineering
ISSG	Interoperability Senior Steering Group
IT	Information Technology
ITS	Imagery Transformation Services
JBMC2	Joint Battle Management C2
JCB	Joint Capabilities Board
JCIDS	Joint Capabilities Integration and Development System
JFCOM	Joint Forces Command
JIA	Joint Integrated Architecture
JITC	Joint Interoperability Test Command
JPO	Joint Program Office
JROC	Joint Requirements Oversight Council
JUON	Joint Urgent Operational Need
KIP	Key Interface Profile
KM	Knowledge Management
KPAs	Key Performance Attributes
KVA	Knowledge Value Added

LAN	Local Area Network
LCS	Life Cycle Support
LRIP	Low Rate Initial Production
MCEB	Military Communications-Electronic Board
MCFI	Multinational Coalition Forces Iraq
MCMTOMF	Mean Corrective Maintenance Time for Operational Mission Failures-Software
MDA	Milestone Decision Authority
MIC	Multinational Interoperability Council
MIDB	Modernized Integrated Database
MLTC	Multi-Level Thin Client
MNIS	Multinational Information Sharing
MS	Mission Secret

NCDOC	Navy Cyber Defense Operations Command
NCES	Net-Centric Enterprises Services
NCOW-RM	Net-Centric Operations and Warfare Reference Model
NCW	Network Centric Warfare
NEC	Navy Enlisted Classification
NDI	Non-Developmental Item
NII	Networks and Information Integration
NLT	Nominal Learning Time
NOC	Network Operations Center
NPS	Naval Postgraduate School
NSS	National Security Systems
NTSP	Naval Training Support Plan

OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OMN	Operations and Maintenance
OSA	Open System Architecture
OS	Operation Specialists
OSD	Office of the Secretary of Defense

PDC	Primary Domain Controller
PEO	Program Executive Office
PIA	Post Independent Analysis
PM	Program Manager
POR	Program of Record
PPBE	Planning, Programming, Budget, and Execution
PRNOC	Pacific Region Network Operations Center
QoS	Quality of Service

RGS	Requirements Generation System
ROI	Return on Investment
ROK	Return on Knowledge
SAAM	Software Architecture Analysis Method
SABI	Secret and Below Interoperability
SADP	
SATCOM	Satellite Communications
SBS	Service Based Sustainment
SECDEF	Secretary of Defense
SEP	Systems Engineering Plan
SEW	Shared Early Warning
SIPRNET	Secret Internet Protocol Router Network
SIT	Shore Installation Training
SME	Subject Matter Expert
SoS	System of Systems
SSAA	System Security Authorization Agreement
SWaP	Space, Weight and Power
TCCC	Theater Communications Control Center
TEP	Theater Engagement Plan
TRAC	Timeliness, Relevance, Accuracy, Comprehensiveness
TSABI	Top Secret and Below Initiative
TTP	Tactics, Techniques, and Procedures
UARNOC	Unified Atlantic Region Network Operations Center
UCP	Unified Command Plan
UCSMO	Unified Cross Domain Management Office
UL	Unit Level
UTC	Ultra Thin Client
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAN	Wide Area Network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to thank Ms. Virginia Bayer, Kenneth Ching, Brian Miller, Michelle Voight, and Jonathan Avis from SPAWAR for their continued help and advice. Their knowledge and encouragement throughout the past year and a half, while we worked on this project was invaluable. We would especially like to thank LtCol Karl Pfeiffer and Mr. Buddy Barreto for their insight, support, and meaningful answers to our many questions. As we stumbled through this process, they were always patient, understanding and eternally helpful no matter what the situation. Lastly, we would like to thank our wives and families for their tireless understanding, resolute help, and unwavering enthusiasm throughout this research.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

CENTRIXS is a standing, global enterprise network allowing U.S. and coalition nations and their forces to securely share operational and intelligence information in support of combined planning, unity of effort, and decision making in multinational operations. When we first proposed our idea for a thesis, the general area of thesis research was to focus on the installation and full deployment of a CENTRIXS network at the Naval Postgraduate School. The development of this network would consist of funding acquisition, hardware and software acquisition, architecting the LAN/WAN network, cryptographic implementation, and information assurance documentation. The focus was on the network-centric use of a secure information medium with government off-the-shelf and commercial off-the-shelf technologies to facilitate effective information sharing and interoperability between the Naval Postgraduate School and all nodes of joint and coalition forces.

Initially, we put together a survey designed to assess the need and desire by the NPS faculty and staff for a CENTRIXS node install on campus. The survey provided questions geared toward gathering information in order to enhance the learning environment and training benefits associated with a CENTRIXS node installation. There is a constant flow of students representing scores of countries that could receive important training by having a CENTRIXS node on campus where they could receive an introduction to the system and become somewhat proficient before returning to their respective commands. Our research team was not prepared for the difficulty encountered in getting the survey to our target group. There are many policy restrictions in place at NPS regarding mass-emailing anything to members of the faculty and staff. Although we had a difficult time administering the survey because of these NPS policy restrictions, those received indicated a need and desire for a CENTRIXS node installation. While distribution and response were less than hoped, we include the survey and related material in Appendix H, and anticipate it will produce a rich data source for future research.

Annually, there are thousands of U.S. officers, combined with scores of international coalition officers who would greatly benefit from the training associated with a CENTRIXS point of presence here at NPS. However, in order to set the foundation for a CENTRIXS node installation on campus, we found that we needed to narrow our scope. This research turned out to be our finished product.

B. OVERVIEW

Through research and study, we attempt to encapsulate thousands of pages of documentation on CENTRIXS, and combine them into a single document that is concise and user friendly. The following paragraphs discuss how we organized this thesis.

We start by defining what CENTRIXS is by illustrating the strategic concept. We discuss the operational, mission, and personnel requirements to help build a picture in the mind's eye of the reader. An architectural description is provided, which contains the system scope, support environment, personnel assessment, and how the end users utilize the system. We conduct an architecture evaluation in order to show ways to improve the modifiability, security, and usability of CENTRIXS networks.

In this research, we also conducted a Knowledge Value Added analysis to streamline the manning and usability of CENTRIXS nodes. We analyzed the current architecture, personnel, and training requirements, then consolidated suggestions on how to improve the system as a whole. Finally, we explore how to efficiently and effectively go through the process of acquisition, installation, and accreditation of a CENTRIXS node and some of the challenges associated with such a task.

II. DEFINING CENTRIXS/ARCHITECTURE EVALUATION

A. INTRODUCTION

This chapter describes the methodology of operating the CENTRIXS networks to support the needs of Combatant Commands (COCOMs) on a global basis. This chapter addresses in general terms who is connected to whom, what kinds of information must be exchanged between users, and the services provided to the users of CENTRIXS networks. "Combined Operations" are defined as those conducted by the forces of two or more nations acting together for the accomplishment of an agreed, common mission.

This chapter also provides an operational overview of the use of CENTRIXS and covers its mission, policies and constraints regarding the use of CENTRIXS, the environment in which it operates, and the groups of people and organizations that are its users. In addition, it also covers the operational needs of the COCOMs dictated by the coalition mission. Finally, it describes the capabilities of CENTRIXS, operational and support environments, and provides illustrations of the employment of CENTRIXS through operational scenarios.

This chapter also explains, in non-technical terms, the COCOM needs for coalition information sharing based on the assumption that most, if not all, future operations involving U.S. forces will require the secure sharing of information with foreign nations and their respective forces. Coalition information sharing between nations and their forces in these combined operations is critical to their success.

We will also describe the theory behind CENTRIXS architecture and evaluate how it works in practice with the use of the Architecture Tradeoff Analysis Method (ATAM). The ATAM will reveal how well the architecture satisfies particular quality goals (such as performance or modifiability), but it also provides insight into how those quality goals interact with each other (Clements, 35, 2002).

Joint warfighting operations demand responsive information exchange across COCOMs and combined forces for planning, unity of effort, decision superiority, and decisive global operations. The overarching warfare requirements supported are: coalition C2; a Common Operational Picture (COP); intelligence, surveillance and reconnaissance (ISR); and coalition information sharing. CENTRIXS is the U.S. global, secure, information network solution to support coalition operations with shared, combined command, control and intelligence information.

B. PROBLEM CHARACTERIZATION

The CENTRIXS is a coordinated Department of Defense Program established at the request of the Combatant Commands (COCOMs) to support the Global War on Terrorism (GWOT). CENTRIXS is a common set of networks built on a set of standard hardware, software, and services. Due to today's policy, operational, and technical limitations, each of these CENTRIXS networks operates at a single security classification level. These networks operate globally, regionally, and locally; in addition, some of them have many members, some have fewer, and some are bilateral in nature. The consistent thread is that they are built to the CENTRIXS standard so that they are essentially "plug and play" anywhere in the world (Boardman, 2, 2004.)

Today, CENTRIXS uses certified and accredited guarding technology to connect some of these networks together and with U.S. networks, but these connections are very restricted and, by their nature, difficult to manage. CENTRIXS consists of a collection of coalition wide area networks (WAN) known as "enclaves" which include CENTRIXS Four Eyes (CFE), for the United States, Australia, Canada and Great Britain; CENTRIXS-J for the United States and Japan; and CENTRIXS-K for the United States and Korea (U.S. Navy homepage, 2007.) In most cases, users must have a separate workstation for each network enclave. The establishment of additional CENTRIXS networks is determined by the demands of the particular exercise or world situation. CENTRIXS is exploring advanced techniques and technology to allow users access to several networks of different classifications from a single workstation.

CENTRIXS networks are globally interoperable and interconnected, relatively inexpensive, and easy to use, built with existing, readily available, commercial technology. Interoperable and interconnected means that all required users for any particular CENTRIXS network can exchange the appropriate information with each other. Inexpensive means that limited resources are required to build the CENTRIXS networks. "Easy to use" means that generally anyone who is familiar with simple office suite software and the use of a browser and an e-mail client can easily learn to use any CENTRIXS network.

C. STRATEGIC CONCEPT

The CENTRIXS is designed to meet the immediate operational needs of the Combatant Commands, allowing them to share information with coalition partners (nations and their forces) in the Global War on Terrorism and other rapidly developing military contingencies. Global CENTRIXS refers to the inter-linking of the various CENTRIXS Enterprise networks (enclaves) at the COCOMs, by the global CENTRIXS Network Control Center (CNCC) (Boardman, 2, 2004.)

Once a mission is assigned to or assumed by a COCOM that requires a coalition information-sharing network, the Command will consider the use of those existing CENTRIXS networks to which it already has access. If possible, an extension of existing networks will suffice; in others, it may be possible to use techniques (like virtual private networks (VPN)) to establish a separate channel over a particular network consisting of a sub-set of that network's authorized users; and as a last resort, the Command can consider initiating a separately encrypted CENTRIXS network at a new security classification.[1]

If applicable, the CENTRIXS network chosen would be used to link the planning of the COCOM with the planning elements of its components as well as the coalition forces that will participate. In addition, there may be a need to connect the Ministries of Defense of these nations, their forces, and sources of intelligence (either U.S. or coalition) to support the planning. Planning activity conducted over the CENTRIXS

[1] This calculation should be made by the Commander based on a risk/benefit ratio. New, separately encrypted networks are costly not only in dollars, but also in response time and manpower. If an existing network can be used, the Command can expect a more rapid network buildup, less cost to be incurred, and require fewer personnel to maintain them. This should also be a result of the commander's consideration of the risk to the operation and information; a risk management decision which properly resides at the highest level within the Command.

network should include (but not be limited to) force contribution coordination; mission, strategy, and campaign planning; basing and transportation; logistics; intelligence sharing; rules of engagement; as well as the initial operational planning necessary for force entry and engagement (Boardman, 3, 2004.)

The goals of the before mentioned applicable CENTRIXS concepts are as follows:

- Enable Coalition Information Sharing: The primary objective of CENTRIXS is to enable secure, coalition information sharing between U.S. forces and those of nations cooperating in military operations. This involves every aspect of information sharing to include relevant operations and intelligence information and data, various security levels, discrete separation of various operational communities within the same virtual network, and all the various mechanisms for exchanging information (email, voice, web "push" and "pull" techniques, chat, *et al*.). These mechanisms cannot be "one way" only (i.e., from U.S. to foreign nation), but must accommodate bi-directional capabilities. Considering the nature of these exchanges, secure interfaces must be available to the participants in order to encourage their willingness to share.
- Coalition Interoperability: Interoperability of U.S. systems with those of coalition partner nations is a key objective of CENTRIXS. CENTRIXS is designed to be the U.S. standard for secure, network connectivity to achieve interoperability in any coalition situation, whether it is an alliance, a coalition, a bilateral or multilateral operation. Open systems specifications for hardware and software are desired in order to facilitate the ability to interoperate. Hardware and software should be COTS products rather than special purpose-built products that serve only one specific user. At the application and systems level, proprietary solutions should be avoided and international standards (e.g., the ISO); W3C should be used whenever possible.
- Seamless, Flexible Connectivity Worldwide: Seamless, flexible connectivity worldwide is required so that U.S. and multinational forces from any part of the World have the ability to interoperate regardless of location. "Seamless" refers to the ability of one CENTRIXS user to exchange with another user with little concern for the physical or virtual path of the network. "Flexible" refers to the ability to quickly reconfigure CENTRIXS to meet the rapidly evolving and emerging needs of combatant commands and their coalition partners. "Worldwide" refers to the ability of CENTRIXS-equipped forces to "plug and play" in any region of the World.

- Availability When Needed: Connectivity to the CENTRIXS infrastructure must be immediately available when a U.S. force needs a secure network to exchange information with a coalition partner. The rapidly evolving international environment presents situations that are generally unpredictable not only in space and time, but also in the participants. In order to meet this objective, CENTRIXS must be accessible through all of the COCOMs and be extendable to the appropriate objective areas and participant nations in a timely manner.
- Protect Information For CENTRIXS Users: Finally, protection of the information that is exchanged over CENTRIXS must be protected from unauthorized access to enable and encourage the exchange itself. In addition, CENTRIXS must provide for the further ability to provide discrete separation of information exchanges within the same virtual networks. This includes the ability to protect information exchanged one-to-one; one-to-many; many-to-many; and between specific groups and/or nations; while still preserving the ability to share with a larger group on a general level.

CENTRIXS is differentiated from the overall Multinational Information Sharing (MNIS) Program of the Department of Defense (DoD) in that CENTRIXS responds to the immediate operational needs of the COCOMs today and is designated a legacy system. MNIS (as proposed) deals with the development of future multinational information sharing systems and capabilities. When MNIS capabilities are successfully fielded within the Global Information Grid (GIG) Enterprise Information Environment (EIE), it is expected that CENTRIXS will be subsumed in some manner by MNIS. Until that time, DoD components will use CENTRIXS for their coalition information sharing needs (unless an exception is granted) in accordance with the instructions and directives of the DoD (Boardman, 8, 2004.)

CENTRIXS is co-sponsored by the Assistant Secretary of Defense for Networks and Information Integration (ASD (NII))/DoD Chief Information Officer (CIO) and the Deputy Under Secretary of Defense for Intelligence (DUSD(I)). The CENTRIXS Program Management Office (CPMO) functions as an activity under the ASD (NII) and the USD (I) to manage CENTRIXS until such time as future Multinational Information Sharing (MNIS) systems are fielded and can replace CENTRIXS (DoD Directive 5137.1, 5, 1992.)

COCOMs use CENTRIXS to connect partner nations in a prescribed Area of Responsibility (AOR) to improve coalition information sharing capability with those nations. The relatively low cost and simplicity of the system is attractive to coalition nations, thereby increasing participation from both the COCOM and allied nation partners. It is important to understand that CENTRIXS is a C2 network made up of many parts, which include fixed and deployable workstations.

CENTRIXS provides the means to share classified information with coalition nations and their military forces. With few physical limits on where the network can be extended, CENTRIXS supports not only the forces directly involved in the combined operations, but also allows for all of the supporting commands and agencies at every operational level to be connected as well. A fully developed CENTRIXS network can connect authorized users around the world in support of combined operations (See Appendix A.)

CENTRIXS uses the U.S. SIPRNET backbone and generally does not require its own communications infrastructure. However, in some cases additional commercial or coalition nation circuits can be used to extend the network to required locations. To protect the SIPRNET from malicious attacks, procedures, computer hardware and software, and guards are in place to prevent attacks that may originate from CENTRIXS.

CENTRIXS can be used for global coalition networks or for smaller coalitions or even bilateral connections. When used for a bilateral network, the connections for CENTRIXS usually run through the office of the Defense Attaché of a U.S. Embassy. In other cases, it may run directly to the Ministries of Defense of partner nations.

CENTRIXS networks can use a series of guard devices that allow information to flow to and from U.S. secure networks without fear of compromising the U.S.-only network. Hardware and software guards, where required, in addition to foreign disclosure procedures and information sharing agreements, ensure the security and integrity of the systems and information (NDP-1, 22, 2002.) Table 1 on the next page provides a list of various enclaves, their locations, and descriptions.

Table 1. Enclave Descriptions

Enclave	Information Exchange
CENTRIXS Four Eyes (CFE)	Australia, Canada, United Kingdom, United States
CENTRIXS – J	United States and Japan
CENTRIXS – K	United States and Korea
CENTRIXS Global Counter Terrorism Force (GCTF)	73+ Nations
CENTRIXS GCTF-COI	Countries that have Communities of Interest (COIs) within the broader GCTF (i.e., Combined Naval Forces CENTCOM, Coalition Force Pacific)
CENTRIXS Multinational Coalition Forces Iraq (MCFI)	~52+ Nations
NATO-Mission Secret (MS)	NATO
United States SIPRNET	U.S. only
Established as required	*Concurrently Operating COIs*

D. OPERATIONAL REQUIREMENTS

COCOMs have an operational need for coalition information-sharing environments where information is shared at the appropriate security levels with partner nations and their forces. This environment supports the processing, storing, and transmission of releasable information from pre-hostilities through post-combat operational planning and execution. Only participants of the coalition operation are allowed access within the coalition information-sharing environment, which also has the ability to share information with other systems as required.

As situations warrant, COCOMs will assemble dynamically changing coalitions in response to assigned mission requirements. C2 networks to support these coalitions will need to be flexible and dynamic in order to respond to the commander's mission needs. This means that the networks should be easily established, changed, and eventually disestablished as requirements change.

In general terms, national policy dictates what information can be shared with coalition partner nations and their forces for specific operations. Under normal circumstances, coalition information sharing will include all information that commanders need to plan and execute operations and to protect the forces in the AOR. It should be noted that the COCOM Commander has broad authorities for the emergency release of information that affect U.S. and foreign forces within his AOR in accordance with assigned missions (NDP-1, 24, 1992.)

U.S. forces are accustomed to using U.S.-only networks for C2, intelligence, and logistics in planning, training, preparing for, and executing military operations. When faced with the requirement to interoperate with coalition forces, COCOMs often resort to ad-hoc methods to exchange information with foreign partner forces. However, when the scope of the operation and the participation of foreign nations' forces increase in importance, combined commanders require solutions that allow them to seamlessly interoperate with coalition partners. When the above requirements take precedence, the combined commander often makes the decision to conduct his operations on a coalition network, rather than on a U.S. network. This approach supports coalition interoperability, mission accomplishment, and protection of the coalition forces engaged (DoD Directive 5137.1, 2, 1992.)

As a result of the need to use a coalition network, commanders often find themselves unable to share some of the information to which they and their forces are normally accustomed to accessing via a U.S.-only network. In many instances, provisions have been made for the transfer of critical information using guarding technology for finished information products, some databases, real time data, limited email, and situational awareness displays in many instances. In many cases, there is still the requirement to have material reviewed by a Foreign Disclosure Officer (FDO) or his representative prior to release of the information to the coalition networks either in an automated manner, or using conventional “sneaker-net” techniques (NDP-1, 61, 2002.)

In some instances, commanders use more than one coalition network due to the limits imposed by policy and technology. Today, each CENTRIXS network operates at an assigned security classification level based on the information exchange requirements and the coalition membership. Although the means to pass information from one network to another exists, it is limited in nature and manpower intensive. An example of this need is when a coalition of nations supports the overall mission, and another set of nations, operating in the same area has agreements to share additional information not available to the larger group. Technology will offer only a partial automated solution to this problem.

CENTRIXS is installed on surface ships (afloat variants) and at the Navy's Regional Network Operations Centers (NOCs) (shore variants). Working together, the afloat and shore variants provide the core data services (i.e., web replication, secure e-mail, collaboration, COP, chat) and access to allied/coalition networks via established firewalls and Cross Domain Solutions (CDS) (See Appendix B.)

Shore variants will reside at the U.S NOC and at the respective Coalition Network Operations Center. The shore variant serves as the gateway between specific CENTRIXS enclave users afloat and allied/coalition networks (See Appendix C.)

Afloat variants must connect to the shore variant located at a NOC. Underway, surface ships will use the ADNS to coordinate Wide Area Network (WAN) transport over various SATCOM links. The Integrated Shipboard Network System (ISNS) provides the ship's internal Classified (Secret High) local area network (LAN.) CENTRIXS afloat variants consist of multiple security enclaves with multiple coalition Virtual LANs (VLANs) that reside on the Classified LAN (See Appendix D.)

Coalition warfare brings its own set of unique operational constraints for the COCOM. These include, but are not limited to (DoD INST 8110.1, 7, 2004):

- Capabilities: The informational, operational, and technical capabilities each nation brings to a coalition will be different. Participating nations must understand the constraints on information sharing and agree to a C2 Interoperability Board (CCIB) process, established by the Regional COCOM, to govern coalition information sharing networks in order to make the CENTRIXS concept of operations viable. The CCIB process will validate command needs and address issues that cannot be resolved at lower levels.
- Security (Releasability/Dissemination): In a coalition environment, the protection of classified information is paramount. Each coalition partner is responsible for establishing and maintaining a secure interface between their national systems and the CENTRIXS networks. In addition, each nation is responsible for protecting the shared information and the coalition information-sharing network from access by unauthorized

persons or organizations. CENTRIXS networks that are within U.S. control will be certified and accredited using the approved processes for the information assurance of information systems.

- Multiple Security Domains: In combined operations there may be a need for more than one coalition security domain that will require more than one coalition information-sharing network. Managing multiple coalition networks as well as the release of information to them will present a challenge to the COCOM. In addition, necessary interaction between these multiple coalition networks and U.S. networks will call for innovative operational processes to facilitate the accomplishment of the coalition mission.
- Foreign Disclosure: Coalition member nations will adapt their foreign disclosure policy to support the sharing of appropriate information with their coalition partners. It should be the default position that information that will affect the accomplishment of the shared mission and protection of coalition forces will be shared as quickly as possible with coalition partner nations by the most rapid means, usually the coalition information sharing network, CENTRIXS.
- Information Throughput Capacity: Participating nations must provide adequate capacity to the coalition information sharing networks to support operational requirements across the full spectrum of their operations.
- Compatibility of Information Systems: Protocols and other technical interfaces of the various systems will comply with international standards in order to achieve this concept. Incompatibilities will be addressed and resolved within the CCIB processes.
- Political Factors: Political considerations are significant at every step of coalition operations. However, once a coalition is formed, mission accomplishment and protection of the coalition forces must be elevated into the foreground to support the agreed mission. Coordination at the strategic/operational level will be necessary to make the coalition information-sharing requirement viable.
- Agreements Between Members: Members of the coalition may have pre-established agreements for information/intelligence sharing. These agreements will be addressed and resolved bilaterally or within the CCIB process as required.
- Policies: Coalition operations work within established policy guidelines. Any issues with existing policy will be documented with proposals for change to support a combined operation. These suggested changes may be handled in national channels or within the established CCIB process, as appropriate.

- Language: Coalition operations always introduce the challenge of language capabilities for the combined forces. Some of these challenges can be addressed partially with technology using language for chat or document translation. However, considerable planning must address this critical area in practical terms and in view of the envisioned combined C2 processes. As a practical matter, English will be assumed to be the default language for CENTRIXS-supported operations.

E. MISSION REQUIREMENTS

Operation Enduring Freedom (OEF) demonstrated the need to share relevant information between coalition partners conducting the full spectrum of combined military operations. When coalitions are established, coalition information-sharing requirements are identified and vetted collectively by coalition members. Limiting factors to be initially considered are bilateral agreements, foreign disclosure requirements, individual participants' information technology capabilities, foreign material sales agreements, and the ability to release (loan or sell) communications security devices.

To achieve economies of scale in coalition systems and solutions, a structured process prioritizing common coalition information exchange requirements is necessary. The C4I (Command, Control, Communications, Computers and Intelligence) information exchange requirements (IERs) for real-world operations have been identified, and are being assessed and validated for coalition forces. Coalition partners will compare the long-term interoperability requirements to the IERs using the CCIB (or similar) forum. Each participating nation will establish formal mechanisms in accordance with their national policies and procedures for the release of information to the other participating nations. Commanders will decide what information is to be shared based on the requirements of the mission assigned (USCENTCOM, 10, 2003.)

Access to information needed to conduct full spectrum operations is controlled, as determined by each coalition member nation's overall level of participation and need to know. Not all information will be shared with all partners; however, it is critical that the default be to share rather than to withhold. The decision to withhold information should be largely determined based on the risk to successful accomplishment of any mission and protection of the combined operational forces involved in specific operations.

CENTRIXS will support the secure exchange of classified information under established disclosure policies in a wide variety of physical and virtual environments in accordance with the national directives of the participating nations (USCENTCOM, 10, 2003.)

Security domains on CENTRIXS within the Combined Joint Task Force (CJTF) allow members within a common operational community the ability to access relevant information necessary to support the corresponding operation. These domains facilitate the sharing of released information essential in conducting crisis action planning and mission execution. These domains must provide protection for each participating nation’s classified or sensitive military and/or civilian information. Nations participating in these security domains must ensure information they receive is not compromised. Information that is electronically shared will be classified and labeled appropriately (CENTRIXS CONOPS, 21, 2001.)

The sharing of intelligence information in support of a pending operation is absolutely necessary. Threats to the CJTF are pervasive and may come from a wide variety of sources as demonstrated in OEF. Therefore, each participating nation needs to share information from many sources including law enforcement, economic, political, infrastructure, organizational, or military perspectives to enable coalition operations to achieve rapid success using the appropriate level of resources. Analysis of this fused intelligence will ensure national assets provided by each participating nation would best be used to disable the adversary. Development of coalition operational plans based on a broad spectrum of all source intelligence enables the right force levels to be employed in theater to be operationally successful while limiting the joint force commander’s force protection and logistics problem (USCENTCOM, 18, 2003.)

The United States and other nations have standing agreements with other alliances and coalitions to include bilateral and multilateral agreements. In the coalition information-sharing environment these agreements must be upheld when a CENTRIXS network is fielded. Emphasis in the production of information, especially intelligence, should be on the content and not on the sources or technical capabilities used to collect or develop it. To allow rapid reprioritization of assets to meet future objectives in on-going operations, post mission assessment must be available in the coalition information-sharing environment. All members have to be able to evaluate (at any given time) the progress of the operation to best apply the assets they have committed (CENTRIXS CONOPS, 43, 2001.)

The 24-hour, 365-day operation of the CENTRIXS network provides connectivity and access within each nation at the appropriate level while maintaining the established security requirements of each participant. Secure connections between the CENTRIXS network communication backbone and existing national C2 (Command and Control) systems are provided as appropriate. Maintenance of the CENTRIXS network is the responsibility of the coalition nations subject to negotiation of the participants. No single nation should be the sole source for maintaining CENTRIXS; generally each nation will maintain its own CENTRIXS systems. The coalition information-sharing environment is capable of global operations as required. Therefore, CENTRIXS networks are interoperable and connected (as appropriate) at some level with other networks (Boardman, 17, 2004.)

CENTRIXS is implemented as a set of secure networks; a set of common applications; a set of common Tactics, Techniques and Procedures (TTP); internationally-accepted encryption capabilities; standardized information formats; and required categories of information for exchange with coalition partners supporting a full spectrum of operations worldwide. It supports education and training for operational and tactical staff planning, leveraging the principles of distributed learning such as specific standards and architecture. It takes advantage of commercially available systems to execute global operations in accordance with the GIG Architecture. The ability to exchange near-real-time information is scalable, deployable, and adaptable for the type of information services required of a CJTF (CENTRIXS CONOPS, 11, 2001.)

F. PERSONNEL REQUIREMENTS

Users at all levels (strategic, operational, and tactical) and of all functional areas (e.g., operations, intelligence, logistics) of CENTRIXS require the ability to interact with all members of the combined military forces using the CENTRIXS capabilities.

Additional capabilities can be provided using CENTRIXS networks based on the individual requirements of the COCOM/Combined Command or their Components to support air, land or maritime combined operations.

Authorized use of CENTRIXS includes planning and preparation for, and execution of combined military operations. All functions of military operations are addressed: personnel, intelligence, operations, and logistics. These activities will include (Boardman, 2004):

- Operational Planning: Those activities involved with identifying, marshalling, and organizing assigned combined forces and with the collection, management, and sharing of intelligence to support this planning and preparation for combined military operations, as well as planning for their employment. These would include operations, intelligence, and logistics planning documents.
- Direction and Redirection of Forces: Those activities associated with executing operational plans and contingencies during combined military operations. These would include operations orders as well as fragmentary orders.
- Reporting of Events and Activity: Those activities involving the reporting of activity in a near real time and non-near real time manner, such as operational, intelligence, and logistics reporting.

G. ARCHITECTURE DESCRIPTION

In all views of the CENTRIXS architecture, certain basic principles and concepts will govern design and implementation. These principles are (Boardman, 2004):

- Regional Organization: CENTRIXS is a global system that is regionally organized and connects the Regional COCOMs (i.e., USCENTCOM, USEUCOM, USNORTHCOM, USPACOM, and USSOUTHCOM) in a secure virtual coalition network. U.S. and coalition nations and forces are connected to these regional commands as appropriate; in addition, other agencies and organizations are connected to the most appropriate CENTRIXS point of presence (CENTRIXS CONOPS, 14, 2001.)
- Centralized Management - Delegated Implementation: The CENTRIXS configuration and its associated standards are centrally managed by the CPMO, but operational implementation has been delegated to the COCOMs. The global CENTRIXS physical infrastructure (the connections between COCOMs) is managed by the Defense Information Systems Agency (DISA).

- Open Systems Architecture is integral to the design of CENTRIXS. The use of this design approach will allow for modularity in CENTRIXS evolution in response to the requirements of its users. The ability to respond to new technologies, new requirements, and new operational environments demands an open systems approach that permits flexible and responsive change to this environment.
- Use of COTS rather than Proprietary solutions: A global system which is interoperable not only with a wide variety of U.S. entities, but also with changing groupings of multinational partners, at all levels of warfare (strategic, operational, tactical), cannot be tied to the limitations that are represented by proprietary solutions. Wherever possible, Commercial off-the-shelf (COTS) and Government off-the-shelf (GOTS) are used in lieu of proprietary solutions. In particular, the interfaces and data exchange standards must be open to the extent that varying users (U.S. and Coalition) can select their own solutions, but still interoperate with others using CENTRIXS.
- Use of International Standards: International standards are the guideline in a system that has coalition users. For example, standards for web activity and data exchange (such as HTML and various versions of XML) will use the standards set by the W3C so that the greatest number of users can participate and evolve as these standards evolve. In addition, various ISO standards will be used whenever possible so that the greatest number of users will know "what the rules are."

1. System Scope

CENTRIXS provides a coalition C2 capability for any combined operation involving U.S. forces. CENTRIXS provides a standard set of COTS and GOTS software. These applications provide core services to include (Boardman, 12, 2004):

- Microsoft Office: Microsoft (MS) Office is the standard tool for creating and editing textual and spreadsheet documents and graphic presentations. MS Office is a suite of software applications that includes MS Word, MS Excel, MS PowerPoint, and MS Outlook. MS Word is used for textual documents, MS Excel for spreadsheets, and MS PowerPoint for presentations and briefings.
- Web Browsing: Netscape and MS Internet Explorer are the web browsing applications operators can use to navigate the CENTRIXS web. The CENTRIXS web server is populated with finished operational documents and intelligence products.

- E-mail: MS Outlook is the application used to pass e-mail between CENTRIXS users via a secure intranet or the SIPRNET in order to exchange information quickly and securely. E-mail is a fast and easy way for users to communicate information and coordinate activities with one or more participants at once.

- Collaboration: CENTRIXS collaborative tools are used to provide coalition members a quick and easy way to conduct real-time business over great distances and with many participants. MS NetMeeting is used as the collaborative tool for CENTRIXS, but other COTS products are also in use (i.e. Voice over Internet Protocol (VOIP) and whiteboard services). To facilitate information sharing among CENTRIXS users, a file sharing system can be established. In addition, secure voice telephones can be supported over CENTRIXS; in combined operations, this is often the only means available of this type.

- C2 Personal Computer (C2PC): The C2PC is a Windows map-based application supporting the Platform Track component of the SADP. C2PC allows CENTRIXS users to view and filter the SADP data tracks, regardless of origin, to better suit specific needs and missions. The display provides:

  - Locations and available status of friendly, neutral, and enemy assets.

  - Planned movement information for friendly, neutral, and enemy assets.

  - Information that could impact the disposition of friendly, neutral, and enemy assets (e.g., weather, Battle Damage Assessment (BDA.)

  - Operator generated features and projections such as operating zones, friendly and enemy activity, air corridors, and missile engagement zones.

  - Force position projections.

- Releasable Modernized Integrated Database (MIDB): An extract of the theater-level and national agency-produced U.S.-only classified MIDB.

- The Imagery Transformation Services (ITS): To store and provide links to releasable nation and tactical images. ITS allows rapid access, query, and manipulation of these images, thus providing tactical operators and intelligence analysts better insight into current and future operations.

2. Support Environment

Hardware and software for CENTRIXS consists of a standardized combination of GOTS and COTS materials, all of which are available and releasable to foreign partners for purchase, lease, or loan. It is imperative that the forward deployed site personnel be qualified to carry out the routine functions of installation, operations, and maintenance for these networks. To ease the burden on the forward deployed personnel, the more complex, difficult functions have been centralized to areas under less stress that are staffed with support personnel with a higher level of training and expertise. In some cases this centralization will be to a deployed Theatre Communications Control Center (TCCC), and in other cases, the COCOM or to the CNCC as appropriate.

The support environment includes network control centers located at the global CNCC, and at each of the COCOMs (DoD Instruction 8110.1, 7, 2004.) The CNCC primary functions include:

- Provide Global Services
- Global Monitoring & Tuning
- Secure the Network & Detect Intrusions
- Provide Connections (Cross-Command and to other government organizations)

The global services to be provided by the CNCC are:

- Root Domain Name Service
- Global Address List Synchronization
- Virus Signature Updates
- Patches & Software Updates
- Cross-Command Services (e-mail, collaboration, search engine)

The support concept mirrors that of traditional automated networks. There are basically five entities in any support plan; the site administrators, the NOC, the TCCC at each of the COCOMS, the CENTRIXS Enterprise support Team (consisting of help desk and support network/systems engineers), and the CNCC.

3. Personnel Assessment

The following summarizes the CENTRIXS jobs and general duties identified as to be the typical fleet defined CENTRIXS manpower requirement:

- CENTRIXS Users: Users are personnel assigned and authorized to perform the day-to-day coalition coordination and communication using the chat, web, mail, COP and collaboration features of CENTRIXS.
- CENTRIXS System Administrators: System Administrators are personnel assigned responsibility for performing very limited network administration, management, net health and analysis of the CENTRIXS system.
- CENTRIXS Web Administrators: Web Administrators are personnel assigned to manage websites and content. They tailor the website's look and feel, how links and postings are managed.
- CENTRIXS Maintainer: Currently the CENTRIXS Maintainer function is defined and assigned to the ISM Technician. Built-in system security lockdowns and very limited administrator permissions restrict users and administrators to only the most basic troubleshooting and repair activities. Network problems beyond the simple re-boot and re-image level will nearly always require on-site technical assistance from CENTRIXS Subject Matter Experts (SMEs) with full System Administrator rights and accesses. Mitigation considerations are:
  - Trained IT technicians are often assigned as System Administrators and would naturally assume the limited troubleshooting maintenance responsibilities if required.
  - Non-technical system administrators, departmental or directorate representatives could safely be called upon to perform the very limited set of troubleshooting and maintenance actions authorized for ship's force.

There is no increase in manpower assessed to be needed at this time. Initial manpower analysis did identify certain CENTRIXS duties. However, it was determined that CENTRIXS fielding adds no additional manpower requirements in the fleet. The workload associated with CENTRIXS implementation is easily offset by the labor savings that this and other new IT systems have generated.

4. End Users

The CPMO provides oversight and management of the engineering, development, integration, and implementation of the CENTRIXS network(s) currently in use by the COCOMs. The CPMO manages the CENTRIXS configuration and is the authority for CENTRIXS networks and systems. The CPMO is also responsible for expanding CENTRIXS connectivity to COCOMs and providing global CENTRIXS connectivity through the CNCC. Figure 1 represents the relationships between the various CENTRIXS entities.

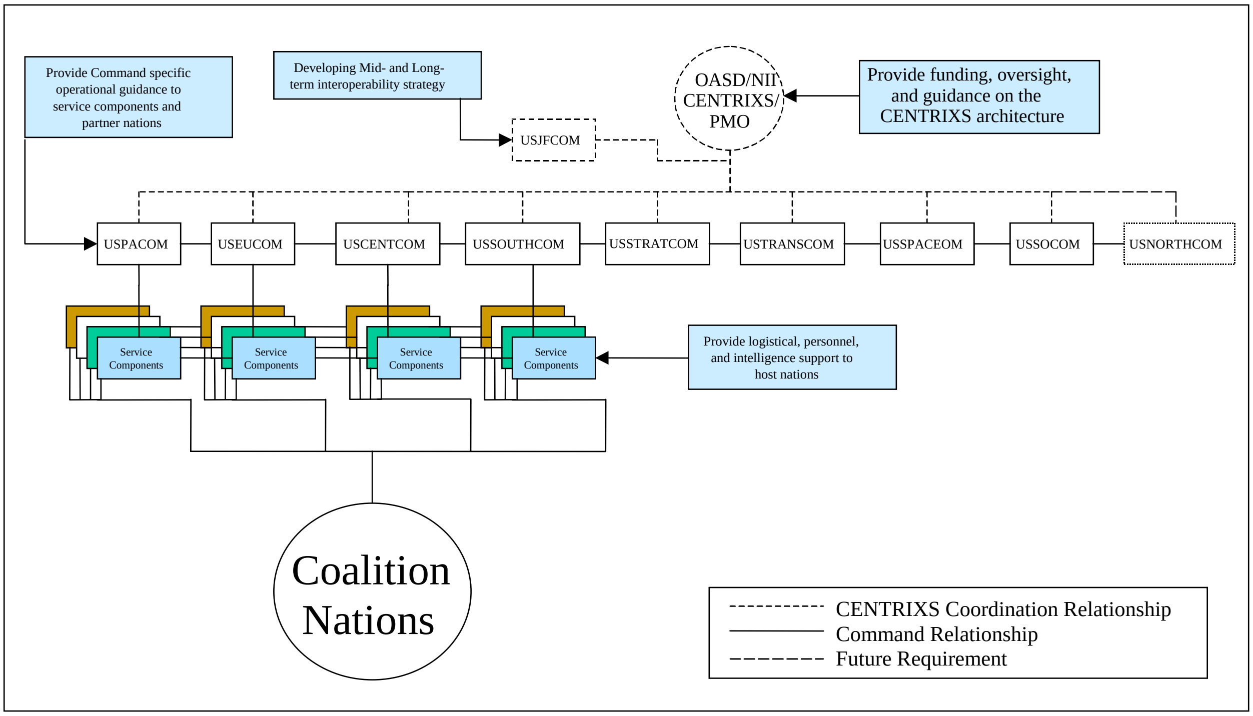

Provide Command specific operational guidance to service components and partner nations
Developing Mid- and Long-term interoperability strategy
OASD/NII CENTRIXS/ PMO
Provide funding, oversight, and guidance on the CENTRIXS architecture
USJFCOM
USPACOM
USEUCOM
USCENTCOM
USSOUTHCOM
USSTRATCOM
USTRANSCOM
USSPACEOM
USSOCOM
USNORTHCOM
Service Components
Service Components
Service Components
Service Components
Provide logistical, personnel, and intelligence support to host nations
Coalition Nations
CENTRIXS Coordination Relationship
Command Relationship
Future Requirement

Figure 1. Command Relationships (From: USCENTCOM, 16, 2001)

The Regional COCOMs, their Components, and nations in their respective AORs are the primary users of CENTRIXS. The JFCOM (Joint Forces Command) also has CENTRIXS installations to support the development of doctrine and procedures, as well as to support experimentation and exercises. Other COCOMs, Components, and Agencies are expected also to request the appropriate CENTRIXS variants so that they may carry out their functional responsibilities. The desired end state is that all COCOMs, Service Components, some National Agencies, and participating nations will be connected to CENTRIXS global information sharing networks. The COCOM/Combined/Component Command J2s, Intelligence Directorates, and their staffs are responsible for providing intelligence-related functional support to assist in the accomplishment of the Command's mission. This includes intelligence operations, training, intelligence dissemination, requests for information, documentation, and requirements management. The J2s provide vision, guidance, and direction for intelligence sharing through CENTRIXS.

The COCOM/Combined/Component Command J3s, Operations Directorates, are responsible for C2 using CENTRIXS. As the Command's coalition C2 network, J3s lead the command's efforts to ensure successful implementation of the CENTRIXS network throughout the command.

The COCOM/Combined/Component Command J4s, Logistics Directorates, are responsible for logistical support using CENTRIXS. As the Command's coalition C2 network, J4s use CENTRIXS to coordinate movement, maintenance, and supply throughout the command (DoD INST 8110.1, 4, 2004.)

The COCOM/Combined/Component Command J5s, Plans and Policy Directorates, are responsible for the Coalition Coordination Cell (CCC). The CCC is made up of both regional and non-regional nations who have demonstrated a willingness to participate with the international community in engagement and contingencies in the COCOMs' AOR. The mission of the CCC is to facilitate strategic/operational integration of coalition forces with U.S. contingency operations in the AOR (DoD INST 8110.1, 5, 2004.)

The COCOM/Combined/Component Command J6s, Communications Directorates, are responsible for designing solutions to stated requirements for CENTRIXS and are responsible for installing, managing, operating, and sustaining their portion of the CENTRIXS networks. J6s will evaluate CENTRIXS requirements and coordinate installation plans with appropriate service components for CENTRIXS networks within their AOR to satisfy those requirements. J6s will also coordinate with the foreign nation to ensure the proposed solution is compatible with their capabilities. CENTRIXS support personnel assigned to deployed locations manage the operation of the forward CENTRIXS gateway(s). Coalition nations are responsible for operation of equipment and systems in their respective national facilities and are responsible for their own communications links to the U.S.-controlled gateways.

U.S. and foreign nation military staffs and their forces will access CENTRIXS either as members of combined headquarters or staffs, or as national forces operationally controlled by a combined force headquarters. Through CENTRIXS, the many coalition partners are able to share classified information through an automated web-based interoperable system, giving the U.S., its allies, and coalition partners the ability to easily share information on a near-real-time basis. CENTRIXS networks are implemented in a way that may be easily expanded when necessary.

In addition to the COCOMs, CENTRIXS is often connected to U.S. embassies in each nation that has CENTRIXS connectivity. The workstations will be installed in the Defense Attaché Office (DAO) and will provide the Defense Attaché (DATT) with a means to stay “in the loop” with the needs of the host nations’ Ministries of Defense (MOD). DAOs can then better facilitate information exchanges between those nations and the COCOM.

H. ARCHITECTURE EVALUATION

In evaluating the CENTRIXS architecture, there are three possible methods, specifically: ATAM, Software Architecture Analysis Method (SAAM), and Active Reviews for Intermediate Design (ARID) (Clements, 33, 2002.) ATAM is the most comprehensive method and is applied after the architecture design approaches have been chosen. It has the advantage revealing how well an architecture fulfills certain quality goals, but also how they interact. SAAM is a less intensive process, where key architectural insights are gained through brainstormed scenarios looking for weaknesses in quality attribute requirements. It is beneficial for quickly assessing many quality attributes of the architecture. Lastly, ARID is used most often during the architecture design and covers the suitability of the design approach (Shannon, 2007.)

The driving architectural requirements, as well as the architectural approaches are discussed in the previous sections. To evaluate the architecture, the functional requirements of CENTRIXS will first be enumerated and the measures of performance and effectiveness specified. The priority quality attributes will be highlighted. In the absence of stakeholder input, scenario-based methods will be used to assess if the CENTRIXS architectural approaches meet the quality attributes it sets out to achieve.

The CENTRIXS high-level architecture diagram (See Appendix B) represents a top-level view of the operational architecture highlighting the interactions between the CENTRIXS architecture and its environment, and between the architecture and external systems. The graphic depicts all CENTRIXS traffic leaving the U.S. and coalition partner ships through satellite communications (SATCOM) to reach the NOCs. As shown, there is no ship-to-ship capability without routing through the NOC. Traffic is instead routed to U.S. forces and coalition partners ashore and afloat from the U.S. and coalition partner NOCs.

The functional requirements in CENTRIXS can be categorized into the following capability areas: (Each function is taken from the Common Systems Function List (CSFL)) (Shannon, 2007.)

- Enterprise Application Support Services
- Perform Briefing and Presentation Services
- Perform Calculation Services
- Create, Manipulate, Produce, and Convert Documents
- Produce and Manage Audio and Graphic Media
- Data Management Services
- Enterprise System Services
- Control Operation of Computer
- Provide Network / Network Application Services
- Provide Transport Services
- Storage Management

A detailed listing of the functional requirements and description are listed below. The key quality attributes of the system, which can be seen in Appendix E, are:

- Performance: The performance quality attribute is with respect to the information domain. The quality of performance can be assessed through TRAC (i.e. timeliness, relevance, accuracy, comprehensiveness.)
- Availability: CENTRIXS must satisfy the definition of operational availability meeting or exceeding the threshold value of greater than or equal to 95 percent and the objective value of greater than or equal to 99 percent.
- Security: CENTRIXS systems must be protected from network attacks by providing a firewall, intrusion detection, virus checking and other Computer Network Defense (CND) functions. The threshold is incorporation and maintenance of network firewalls for each CENTRIXS enclave at the NOCs' boundaries with CENTRIXS Global, installation and regular operation of virus checking systems. The objective is integration of CND functionality into all CENTRIXS systems.
- Modifiability: CENTRIXS, within the hardware support limitations of the afloat variants, must provide tools and procedures for the cost-effective changeover and addition of coalitions. The threshold is manual changeover or addition of coalition enclaves and COIs to CENTRIXS afloat installations. The objective is automated changeover or addition of enclaves to CENTRIXS installations. Each enclave maintains connectivity to other nations and other non-Navy U.S. Commands, Services, and Agencies (C/S/A) participating in CENTRIXS networks. The Defense Information Systems Agency (DISA) operates the CENTRIXS Global network, through which connectivity is provided to other C/S/As and participating nations. CENTRIXS interconnections with the CENTRIXS Global network and in some cases, directly to other nations, are built and maintained at the NOCs.
- Usability: CENTRIXS must be capable of being restored after an operational mission software fault with a threshold Mean Corrective Maintenance Time for Operational Mission Failures-Software (MCMTOMF-sw) time of less than 1.5 hours and an objective of less than 30 minutes. Maintenance personnel must be capable of repairing CENTRIXS after an operational mission hardware fault with a threshold Mean Corrective Maintenance Time for Operational Mission Failures-Hardware (MCMTOMF-hw) time of less than 4 hours and an objective of less than 3 hours. All activity interfaces, services, policy-enforcement controls, and data-sharing of the Net-Centric Operations and Warfare Reference Model (NCOW-RM) and GIG Key Interface Profiles (KIPs) will be satisfied to the requirements of the specific Joint Integrated Architecture (JIA) products (including data correctness, data availability and data processing), and information assurance accreditation, specified in the Threshold (T) and Objective (O) values. CENTRIXS shall meet the threshold value by satisfying 100 percent of the interfaces; services;

policy-enforcement controls; and data correctness, availability and processing requirements designated as enterprise-level or mission critical in the Joint integrated architecture. CENTRIXS shall meet the objective value by satisfying 100 percent of the interfaces; services; policy-enforcement controls; and data correctness, availability and processing requirements in the Joint integrated architectures.

1. Modifiability

Modifiability is the ability to rapidly share information with a dynamically changing combination of coalition forces. This capability must provide for a seamless exchange of C2 information with allied and coalition partners. COCOMs, as situations warrant, will assemble dynamically changing coalitions in response to assigned mission requirements. C2 networks to support these coalitions need to be easily established, changed, and eventually disestablished as requirements change in support of the commander's mission needs. The organization of specific forces assigned, both U.S. and multination, will vary greatly. Under normal circumstances, CENTRIXS will provide the connection to the headquarters of these forces down to the level required by the COCOM. CENTRIXS will allow the secure exchange of information by all elements of these headquarters and units assigned to include operations, intelligence, and logistics personnel required to accomplish the assigned missions of these forces.

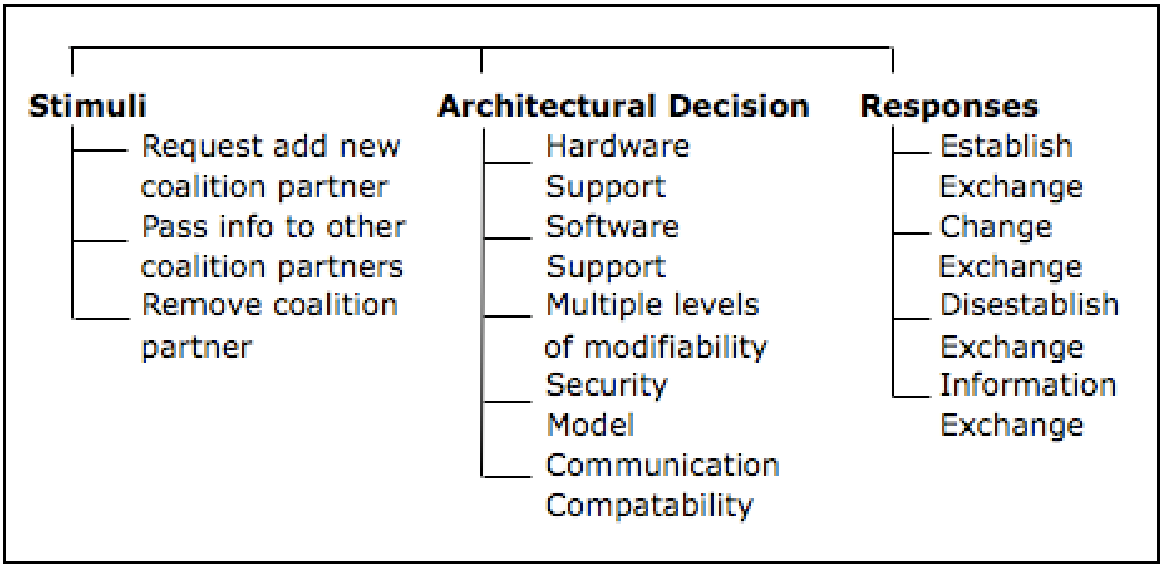


Figure 2. Modifiability Characterization

A current scenario to illustrate the quality attribute of modifiability exists in modern operations in the Middle East. The current solution is for U.S. Central Command (USCENTCOM) to field separate COI networks and individual bilateral networks in support of the war on terrorism and theater specific objectives. The CENTRIXS-GCTF supports Operation Enduring Freedom and has been designated the coalition network for all maritime forces in the USCENTCOM AOR. CENTRIXS-MCFI supports OIF, and is the primary C2 tool/system of record for OIF security and stability operations. CENTRIXS Four Eyes (CFE) supports information exchange between the United States and its Commonwealth allies (Boardman, 11, 2004). Figure 3 shows the various coalitions within CENTRIXS.

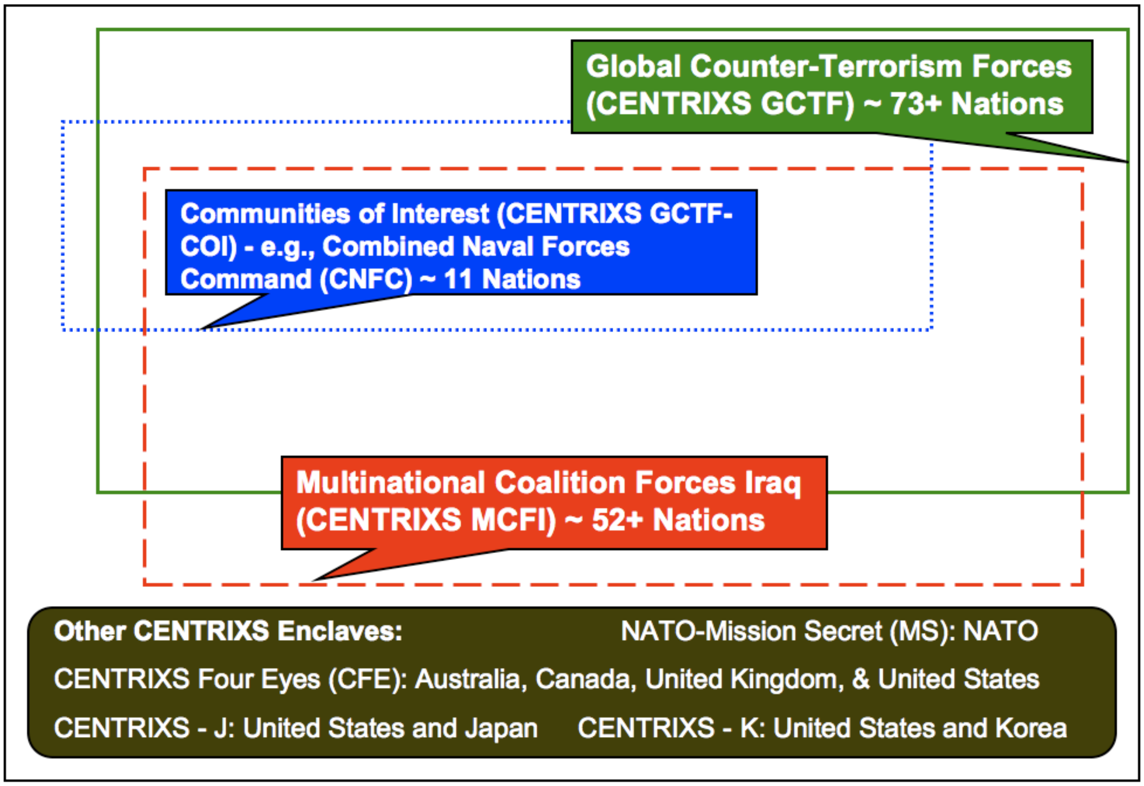

Global Counter-Terrorism Forces (CENTRIXS GCTF) ~ 73+ Nations
Communities of Interest (CENTRIXS GCTF-COI) - e.g., Combined Naval Forces Command (CNFC) ~ 11 Nations
Multinational Coalition Forces Iraq (CENTRIXS MCFI) ~ 52+ Nations
Other CENTRIXS Enclaves:
NATO-Mission Secret (MS): NATO
CENTRIXS Four Eyes (CFE): Australia, Canada, United Kingdom, & United States
CENTRIXS - J: United States and Japan
CENTRIXS - K: United States and Korea

Figure 3. CENTRIXS Coalition Organization (From: Boardman, 12, 2004)

The information sharing challenge exists, as there are no information data exchanges between enclaves. Coalition forces will continue to play a vital role in current and future operations; however, nation organization within the enclaves will continually change. Multiple coalitions, international organizations, and alliances participating in different operations will further complicate the information sharing challenge as well. Analysis performed in this thesis reveals that the need to manage these enclaves is paramount to the success of CENTRIXS.

- Vulnerability: The architecture's current information sharing policies are adequate to handle the various coalition additions and exchanges, however many inconsistencies are discovered. A lack of manageable technical solutions, data owner guidance from various nations, and an onerous accreditation and certification process have all contributed to a lack of seamless data dissemination. This can result in the creation of multiple, separate networks to address these issues that have consumed limited resources and manpower.

- Sensitivity: A key sensitivity for the enclave management and modifiability attribute is the impact on coalition nations as the state of the world changes. With the number of participants in operations throughout the world, it is necessary to minimize the impact on current members while diplomatically removing coalition partners. Political, economic, cultural, technical, and military differences with partners continue to make it difficult for the theater commanders to achieve effective modifiability.

2. Security

As identified by the GIG Integrated Architecture, the consequences of an attack against the National Security enterprises will be far greater than lost Internet transactions (Shannon, 2007.) Through relatively unsophisticated attacks such as viruses, Trojan horses, worms, spyware, and other malicious code, business operations can be, and have been, brought to a halt for hours or even days. This could include the loss and/or theft of data that may never be recovered. Adversaries reading, writing, modifying or destroying information could allow unfriendly forces to influence our decisions or determine our actions before they are executed. The potential consequences of a cyber attack could include denied ability to achieve mission objectives, loss of life, and denied control of U.S. weapon systems (including the possibility of turning our own weapon systems against us).

The projected threat environment in which the CENTRIXS system will operate includes an established and continually growing number of worldwide entities capable of conducting Information Operations (IO). Some subsets of these most likely threats have specific tasking against U.S. communications, networks, and computer systems. Analysis performed in this thesis revealed that a division of IO, Computer Network Operations (CNO), can be further broken down into four categories:

- Compromise-of-Information: When an adversary gains access to allied information either by making an electronic copy of material in transit or by gaining access to the host machine. An example is a network consisting of a secret system and an unclassified system, where secret information exfiltrates from the secret system to the unclassified system. This could occur as a result of operator error, system failure, or a malicious attack.

- Data Deception or Corruption: When the data contained in a system or being transmitted over a data or sensor link is modified (intentional or not). For example, corruption can occur during low to high data transfer if the data on the low side contains malicious code. A compromised low side Web asset that redirects traffic to a hostile nation-state is a form of deception
- Information Denial or Loss: When access to needed information is disrupted. This is typically seen as a denial of service, destruction of transport mechanisms, or signal jamming.
- Physical Destruction or Damage. When the original state of a system's physical components is altered or destroyed. The physical threat for cross-domain networks is the same as for any Information Technology (IT) or Information Assurance (IA) system (Clements, 89, 2002.)

The CENTRIXS system is vulnerable to internal and external threats. These threats could target core functions and the interconnected sensor and communications systems. These threats are worldwide in origin, technically diverse, multifaceted, and growing rapidly. These security threats will be the stimuli in the characterization of this quality attribute. Some of the architectural decisions based on a four-layered approach are also suggested to achieve the goals of availability, confidentiality, integrity, authenticity, and non-repudiation. Figure 4 shows the security attribute characterization.

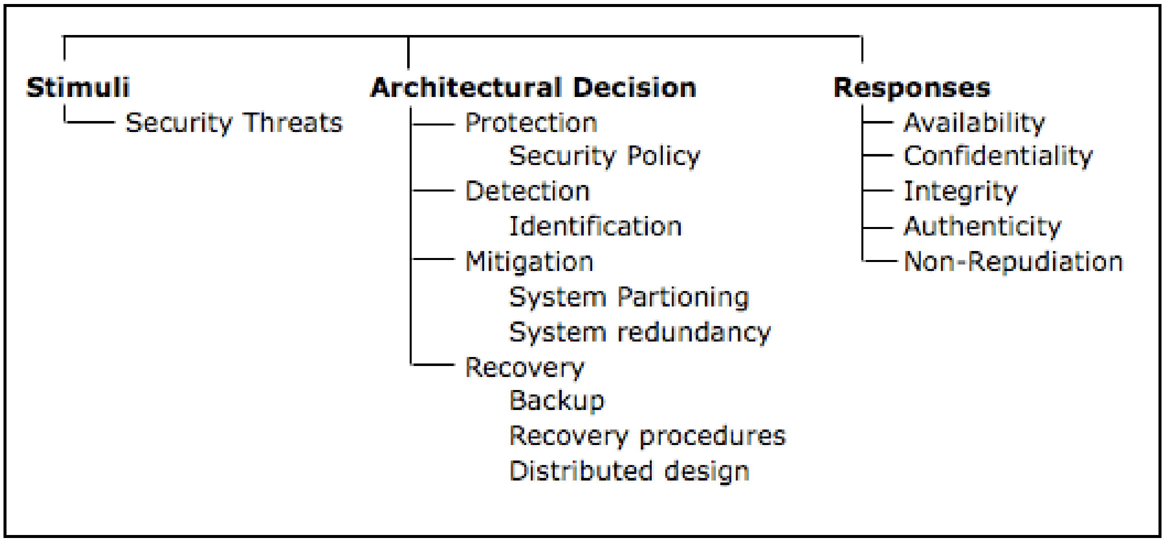


Figure 4. Security Characterization

A scenario-based approach is taken to analyze the quality attribute of security. CENTRIXS incorporates and maintains network firewalls for each CENTRIXS enclave at the NOCs' boundaries with CENTRIXS Global. Also, host and network intrusion detection, as well as virus checking are integrated into all CENTRIXS systems. The CENTRIXS system is currently in full compliance with the DoD Directive 8500.1 and has made the required Information Assurance documentation available to the Joint Staff J-6 for review (Shannon, 2007.)

CENTRIXS employs certified security-enabled information technology to support responsive movement of approved data from U.S.-only sources. This includes e-mail guards for e-mail with the SIPRNET, Radiant Mercury guards for formatted message text data and imagery, Multi-level Database Replication/Security Bridge for Order of battle files and one-way fiber systems for file and database transfers. Standing Foreign Disclosure procedures and training provide the structure and process for approving disclosure and release of data to foreign partners. In our opinion, CENTCOM uses current but limited approved guarding solutions to enhance information flow between the SIPRNET and CENTRIXS.

- Vulnerability: CENTRIXS ought to take special cognizance of the inherent risk of trusted partners within enclaves due to the multiple communities. A more comprehensive security approach needs to be instituted, to provide a seamless, interoperable, multi-classification level information exchange between coalition partners. To transition fully from an air-gapped environment for seamless, robust multilateral and bilateral information sharing, CENTRIXS should expand baseline services and infrastructure to integrate commercial multi-domain and multi-level information exchange capabilities as these technologies are developed, tested, and certified.
- Sensitivity: Technical solutions such as usage traceability and archiving of member logs may be required to allow detailed investigation or preventive auditing. Also, such solutions would need to account for continual updating of the various enclaves.

3. Usability

CENTRIXS must meet relevant MCMTOMF software and hardware requirements, in order to minimize operational down time and maintain availability of CENTRIXS services. In order to achieve the usability goals, Figure 5 illustrates the usability characterization, which employs hardware and software redundancy.

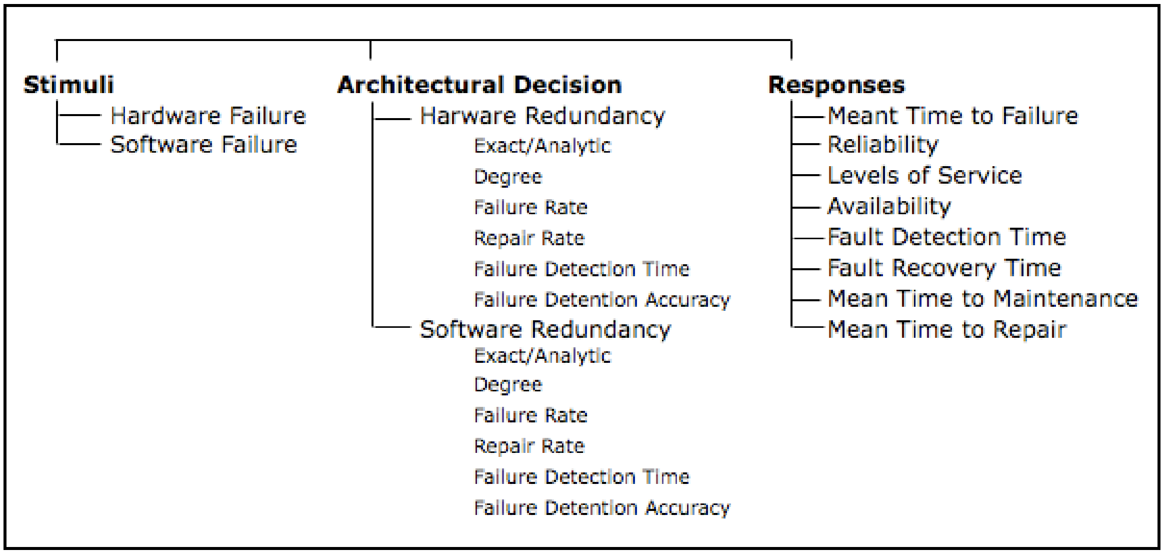


Figure 5. Usability Characterization

There is very little information regarding "how" the CENTRIXS architecture contributes to the Usability objectives. Key Performance Attributes (KPAs) were listed that provided information on the importance of maintaining adaptable and efficient services. Hardware and software redundancy can be assumed to be included in the CENTRIXS systems. The CENTRIXS system shall be fielded in compliance with the IA policies documented in the Department of Defense (DoD) Directive8500.1 and the IA security requirements documented in the DoD Instruction 8500.2. Any unsatisfied IA policies and requirements shall be addressed with an appropriate and corresponding Risk Level (Bayer, 2007.)

- Vulnerability: CENTRIXS is web-centric and commercial off-the-shelf (COTS) focused. Implementation focuses on fielding core information services first, including e-mail, web-based data access, file sharing, collaboration, and near-real time data access. The system is comprised of commercially available computers and network equipment. Redundancy can be achieved efficiently through COTS technologies; however, an entire system may be vulnerable or susceptible to a particular failure or threat. Software applications are both COTS and GOTS. CENTRIXS includes a web-based, multinational-releasable application set to provide the desktop and data infrastructure elements. Due to the increasing software complexity, the CENTRIXS systems are more susceptible and sensitive to bugs. The testing and certification process aims to reduce the probability of a software failure, although is not perfect.

- Sensitivity: The CENTRIXS applications allow the user to access the order of battle and imagery databases and to display the data on a map background. A CENTRIXS workstation user is able to access browser-based products and databases, receive and display track data feeds on a map background, send e-mail with attachments, and conduct collaboration sessions. With coalition operations becoming more prevalent and widespread, the important hardware and software aspects must not be overlooked.

I. CONCLUSION

A developing crisis in the world often results in the requirement for a COCOM to prepare, implement and execute a plan for the potential use of military force to carry out a mission in support of the national interest in accordance with the Unified Command Plan (UCP). Due to dependency on other nations' support for basing, access to airspace, logistic support, and for troop contributions, the COCOM must include these nations in planning efforts. The responsible COCOM and his/her Coalition partners must accomplish those labors together. Through a political process orchestrated at the level of the COCOM, a coalition of nations is formed who have agreed on a common purpose to deal with the developing crisis. In order to enable responsive information sharing with these nations, the use of CENTRIXS is necessary to establish a common architecture for effective operations.

THIS PAGE INTENTIONALLY LEFT BLANK

III. INCREASING THE VALUE OF CENTRIXS

A. INTRODUCTION

This chapter discusses the infrastructure of current CENTRIXS nodes, and suggests changes to those structures in order to maximize their value. Through a detailed analysis and research of the core capabilities of current CENTRIXS nodes and their "AS-IS" processes, this chapter develops the "To-Be" and "Radical" processes and provides a Knowledge Value Added (KVA) analysis in order to suggest ways to improve the nodes' structure and efficiency.

By reviewing and analyzing the documentation provided by PMW-160, we hope to accurately map the CENTRIXS core processes and produce a product, which will assist the program office with completing the acquisition process and will help eventually make CENTRIXS an official Program of Record (POR) at NPS. In order to map the process and determine KVA for the CENTRIXS "AS-IS" process, we will address the following key issues and concerns:

- Identify the core sub-processes, which comprise the CENTRIXS process.
- Identify the average number of personnel required to support a CENTRIXS node.
- Identify both the average number, and types of services produced each day.
- Identify the percentage of total services being provided by each sub-process.
- Create a process flowchart for the "AS-IS", "To-Be" and "RADICAL" processes.
- Create an Excel Spreadsheet in order to calculate KVA for the "AS-IS", "To-Be", and "RADICAL" processes.

Our expectation is that thorough research of the core sub-processes we will be able to determine the KVA for CENTRIXS nodes. PMW-160 is currently focused on obtaining POR status for the system, and is smoothing the Capability Planning Document

(CPD) to go before the Joint Requirements Oversight Council (JROC). Although, this thesis does not directly support the CPD, it should provide useful information regarding the management, services, and value of CENTRIXS.

B. MAKING CHANGES

PMW-160 provided the valuable high-level details required to define the “AS-IS” process and perform a KVA analysis. They provided detailed information such as the number of active CENTRIXS nodes, estimated number of customers per node, and the services common to all customers (Bayer, 2007.) The Networks, Information Assurance (IA), and Enterprise Services Program Office provides information infrastructure supporting client applications in the Command, Control, Communications, Computers, and Intelligence (C4I) networks environment. Figure 6 depicts the service-based architecture with information exchanges between operational nodes both external, and internal to the system. Need lines 1-7 show the external information exchanges across the CENTRIXS boundary between the non-CENTRIXS operators and resources and the CENTRIXS COP, collaboration services, email services, directory services, information repository services, web services and security/account management services.

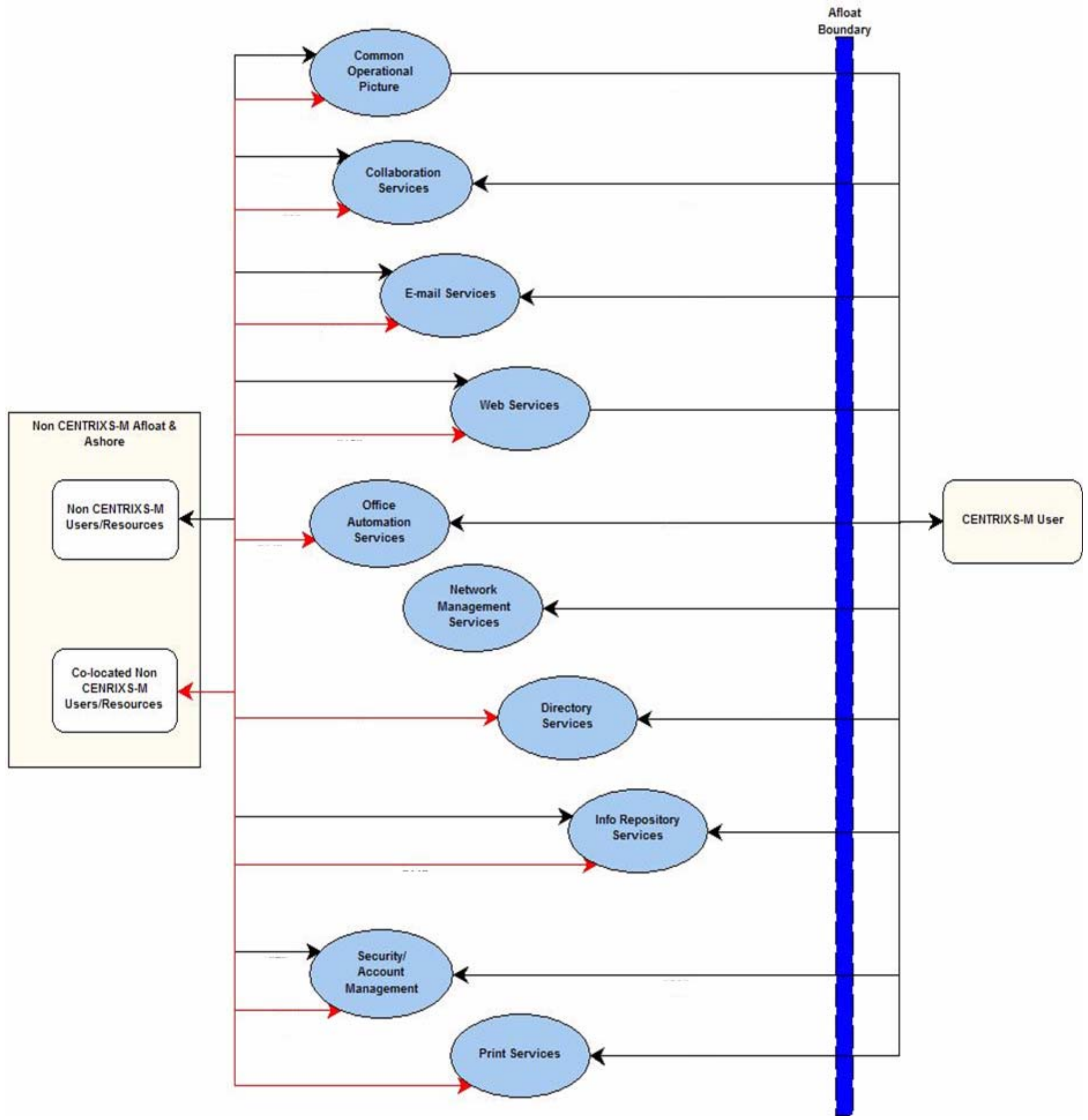

Afloat Boundary
Common Operational Picture
Collaboration Services
E-mail Services
Web Services
Non CENTRIXS-M Afloat & Ashore
Non CENTRIXS-M Users/Resources
Office Automation Services
CENTRIXS-M User
Network Management Services
Co-located Non CENRIXS-M Users/Resources
Directory Services
Info Repository Services
Security/ Account Management
Print Services

Figure 6. Operational Node Connectivity Description Overview

CENTRIXS currently exists as a web-centric, Commercial Off-the-Shelf (COTS) based global network that permits multi-national information sharing. The CENTRIXS core sub-processes provide allied and coalition forces with information services such as e-mail, web services, collaboration, and products such as Global C2 System Integrated Imagery and Intelligence (GCCS-I3) components for the Common Operational Picture (COP), Common Intelligence Picture (CIP), near real-time intelligence, and integrated imagery. PMW-160 is currently managing the acquisition of the critical CENTRIXS system in the Navy's afloat and shore NOC environments as a project until the formal Navy CENTRIXS POR is established. CENTRIXS Increment 1 is proposed to enter the Acquisition cycle as an Acquisition Category (ACAT) III program with a Milestone C decision briefing scheduled for 2nd Quarter FY08. Program Executive Office C4I (PEO C4I) will be the Milestone Decision Authority (MDA) (Brewin, 15, 2007.)

CENTRIXS uses the Automated Digital Network System (ADNS) as the Internet Protocol (IP) gateway to ships and naval shore Operators via current satellite communications (SATCOM) links. The CENTRIXS program incorporates and adapts a variety of COTS hardware and software and GOTS software. Figure 7 illustrates the relationships among organizations or organization types that are the key players in architecture. These key players correspond to the operational nodes, which contain added detail on how the key players interact together in order to conduct their corresponding operational activities.

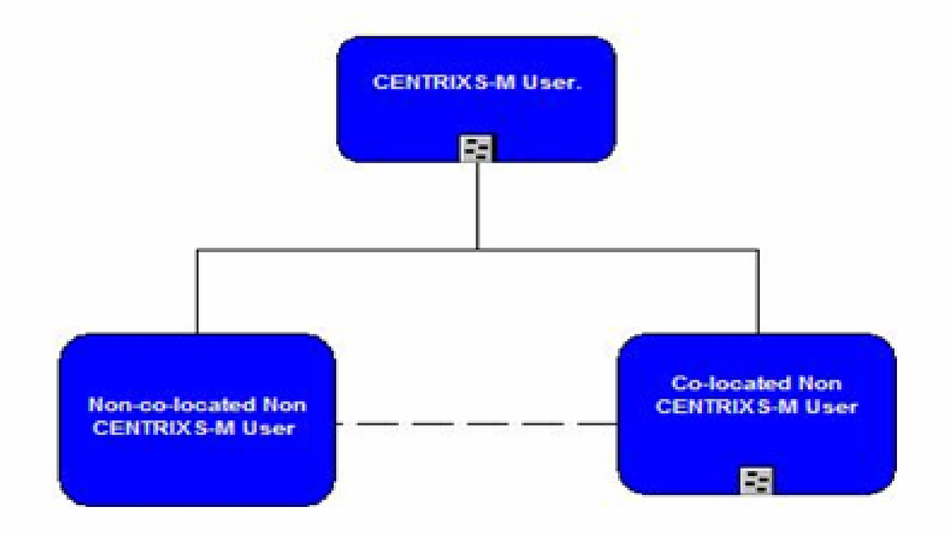

CENTRIXS-M User.
Non-co-located Non CENTRIXS-M User
Co-located Non CENTRIXS-M User

Figure 7. Organizational Relationship Chart Overview

CENTRIXS provides simultaneous access to multiple enclaves using Thin Client System architecture to reduce the Space, Weight, and Power (SWaP) footprint aboard Unit and Force Level platforms (Shannon, 2007.) The design complies with Open System Architecture (OSA) and Defense Information Systems Registry (DISR) guidance to ensure flexibility and interoperability. Through spiral development, successive increments will incorporate new equipment, interfaces, and additional CDS capabilities, which will expand on the capabilities of the CENTRIXS Increment 1 configuration. The ultimate goal is to continue to incorporate CDS capabilities into CENTRIXS to support the transition to the MNIS program (DoD 8110.1, 2004.)

The phone conversations, documentation, and research provided a clear understanding of the "AS-IS" CENTRIXS process. However, the relationship between the core sub-processes, number of services provided, number of customers being serviced, and the manpower required still needed to be correlated. PMW-160 provided additional enlightenment concerning the sub-processes, which made it possible to determine how the sub-processes or services are managed. Therefore, it was possible to view the required enterprise services, the PMW 160 processes, and each node in the system in order to capture the learning time for personnel performing the services, which make up the seven-core CENTRIXS sub-processes. Further, by successfully identifying personnel, roles, training, sub-processes, and the services provided, we were able to determine the KVA. The "AS-IS" process flowchart and KVA Spreadsheets were both constructed using the data provided by PMW-160. Unfortunately, PMW-160 did not have accurate data concerning how often personnel actually performed a service or function, so our team constructed the model based on our extensive experience working on similar systems in similar environments. Figure 8 shows how all CENTRIXS traffic leaving the U.S. and coalition partnerships via SATCOM to reach the NOCs. There is no ship-to-ship capability without routing through the NOC. From the U.S. and coalition partner NOCs, traffic is routed to U.S. forces and Coalition partners ashore and afloat. Figure 9 gives an overview of the core sub-processes of CENTRIXS nodes.

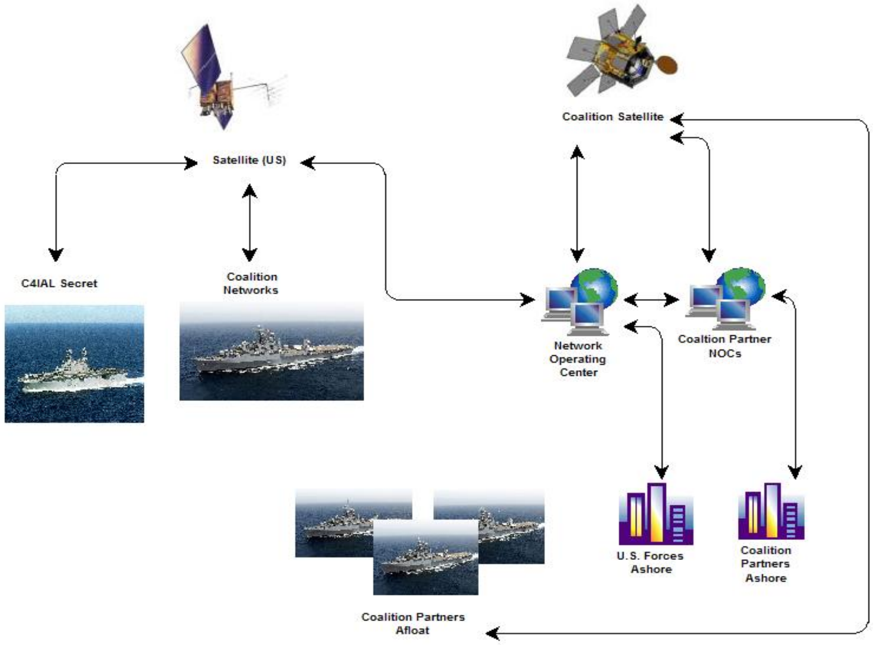


Figure 8. High-Level Operational Concept Graphic Overview (From: Boardman, 2004)

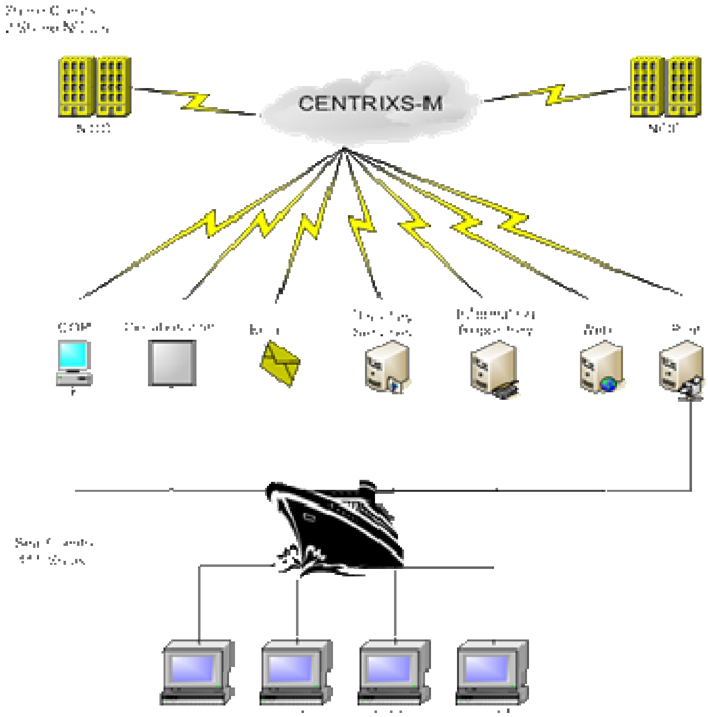


Figure 9. CENTRIXS Core Sub-Process Overview (From: Boardman, 2004)

C. "AS-IS" TRAINING

The following Electronics Technicians (ET) and Information Technicians (IT) courses and their duration, which provide the foundation for CENTRIXS training are as follows:

- A-531-0046 Journeyman Networking Core (**6 Weeks**). This course provides the networking systems foundation training to prepare candidates for management and administration duties on navy networking systems.
- A-150-2300 Information System Maintenance Technician (**12 Weeks**). This course provides general navy network systems troubleshooting and repair training.
- A-531-0022 Network Security Vulnerability Technician (**6 Weeks**). This course prepares trained network administrators to perform security vulnerability duties on navy networks.
- A-531-0045 Advanced Network Analyst **(6 Weeks**). This course provides trained and experienced navy network administrators with advanced training on network management, analysis and troubleshooting.
- A-531-0009 Information Systems Security Manager Course (**2 weeks**). This course provides trained and experienced Naval Officers and Senior Network Administrators with advanced training in the implementation of DoD and Navy Information Systems Security Policies.

These courses award a Navy Enlisted Classification (NEC) that identifies the holder as possessing specific network skills in addition to their normal rating skills. These additional NETC training courses can provide additional indirect training for the CENTRIXS System Administrator, but are not offered as part of the standard CENTRIXS training under the POR (Soriano, AFCEA, 2007). Table 2 shows a breakdown of client variants, and the number of clients and terminals at various nodes.

Table 2. Breakdown of Client Variants, Number of Clients and Terminals

Platform	CENTRIXS Variant	Clients "NODE"	Terminals per Client/Node	Terminals Total
Aircraft Carrier - Nuclear (CVN)	Force Level	8	30	240
Amphibious Assault (LHA)	Force Level	2	30	60
Amphibious Assault (LHD)	Force Level	6	30	180
Amphibious Command (LCC)	Force Level	2	30	60
Amphibious (LPD)	Unit Level	8	15	120
Guided Missile Cruiser (CG)	Unit Level	22	15	330
Guided Missile Destroyer (DDG)	Unit Level	63	15	945
Network Operation Center (NOC)	Shore	2	Variable; (30) As required	60
	Total Clients	**=113**	**Total Terminals**	**=1995**

In addition to the training listed above for ET, CENTRIXS courses are available to enhance the benefits of the normal specialty courses. Table 3 lists critical jobs associated with CENTRIXS and the ratings and associated training time required to qualify for those jobs.

Table 3. CENTRIXS Jobs, Ratings, & Associated Training

PLATFORM	OPS Operators **(75)**	MAINT Maintainers **(4)**	SYS ADMIN System Administrators **(4)**	WEB ADMIN Web Administrators **(2)**	Training Days x Personnel x Terminals
SURFACE **111 Clients**	Install OJT **1 week** JQR/PQS Video **3-4 hr**	ISM NEC **12 weeks** Install OJT **1 week** JOQ/PQS Video **4 hr**	JNC PREREQ **6 weeks** P/O ISNS SM **2 Weeks** Install OJT **1 week** Module **3 Days**	Install OJT **1 Week** Class/lab **3 days**	
SHORE **2 Clients**			JNC PREREQ **6 weeks** Install OJT **1 week** MTT REFTRA **1 week**	Install OJT or MTT REFTRA **1 week** Class/lab **3 days**	
CENTRIXS Training Days per person	**6 Days**	**66 Days**	**48 Days**	**8 Days**	**128 Days**
Prerequisite Training Days per person	**0 Days**	**730 Days**	**365 Days**	**180 Days**	**1275 Days**
Total Training Per Person	**6 Days**	**796 Days**	**413 Days**	**188 days**	**1403 Days**
Total Training Days x number of personnel	**6 Days** **X 75** **450 Days**	**796 Days** **X 4** **3184 Days**	**413 Days** **X 4** **1652 Days**	**188 Days** **X 2** **376 Days**	**5662 Days**

D. "AS-IS" PERSONNEL

A CENTRIXS Manpower Assessment working group identified three jobs, outlined in Table 4, as being required for CENTRIXS operations (Shannon, 2007.)

Table 4. Manpower Assessment

CENTRIXS JOB	TYPICAL RATING/BILLET	# ASSIGNED PER SHIP
OPERATOR	OS, IS, CT, FC, ET, IT, OFFICER	(7 - 200) Personnel = **75 avg**
MAINTAINER	IT, ET, CT, FC	(2 - 6) Personnel **= 4 avg**
SYSTEM ADMIN.	IT, ET, CT, FC	(2 - 6) Personnel = **4 avg**
WEB ADMIN.	IT, IS, OS, OFFICER	(1 – 3) Personnel = **2 avg**

The following summarizes the CENTRIXS jobs and general duties identified, as well as the rating/billet and how many personnel the COMPACFLT training team has found to be the typical fleet defined CENTRIXS manpower requirement:

- <u>CENTRIXS OPERATORS/OPERATORS:</u> Operators are personnel assigned and authorized to perform the day-to-day coalition coordination and communication using the chat, web, mail, COP and Collaboration at Sea (CAS) features of CENTRIXS. ALT = 6 Days.
- <u>CENTRIXS SYSTEM ADMINISTRATORS:</u> System Administrators are personnel assigned responsibility for performing very limited network administration, management, net health and analysis of the CENTRIXS system. ALT = 413 Days (48 specific + 365 core.)
- <u>CENTRIXS WEB ADMINISTRATORS:</u> Web Administrators are personnel assigned to manage websites and content. They tailor the website's look and feel, how links and postings are managed. ALT = 188 Days (8 specific + 180 core.)
- <u>CENTRIXS MAINTAINER:</u> Currently the CENTRIXS Maintainer job is defined and assigned to the ISM Technician. Built-in system security lockdowns and very limited administrator permissions restrict ship and shore forces to only the most basic troubleshooting and repair activities. Network problems beyond the simple re-boot and re-image level will nearly always require on-site technical assistance from CENTRIXS SMEs with full System Administrator rights and accesses. Mitigation considerations are provided below: ALT = 796 Days (66 specific + 730 core) (Shannon, 2007.)

Electronics Technicians are often assigned as System Administrators and would naturally assume the limited troubleshooting maintenance responsibilities if required. While Non-ET system administrators could safely be called upon to perform the very limited set of troubleshooting and maintenance actions authorized for ship and shore forces, there is no increase in manpower perceived to be needed at this time. Initial manpower analysis did identify certain CENTRIXS duties. However, it was determined that CENTRIXS fielding adds no additional manpower requirements in the fleet; only additional training. The workload associated with CENTRIXS is easily offset by the labor savings that this and other new IT systems have generated Ship-wide and Fleet-wide.

As a result of the aforementioned tables and diagrams, it was possible to prepare the KVA analysis and determine the Return on Knowledge (ROK) for the "AS-IS" process. Figure 10 ("AS-IS" Process Flowchart) and Figure 11 (KVA Spreadsheet) represent the relative comparison between the seven core sub-processes/services and measure the knowledge value for each of the sub-processes. The "AS-IS" KVA Spreadsheet derives value from examining the learning time, or knowledge, created, which resides either in the minds of the Operators, Maintainers, System Administrators, and Web Administrators, or the embedded IT. Actual Learning Time (ALT) is defined as the time required to train personnel to perform their role in supporting the seven core sub-processes. The ALT numbers were provided by PMW 160 and are outlined in the CENTRIXS Capabilities Planning Document. However, the prerequisite learning times were also factored in and listed in Table 3. Nominal Learning Time (NLT) is a normally calculated using a second estimate of the knowledge required to perform the sub-processes obtained from a second source. However, in the case of CENTRIXS, we were unable to determine a second source, and therefore did not attempt to calculate NLT. NLT numbers in the figure were derived from the analysis of input obtained from the surveys. Comparing the ALT and the NLT provides a relative ratio between the two, which is an accepted way of validating the ALT. The correlation used for validation of the ALT was any total greater than 80%. If the numbers correlate well, one could assume that there is some statistical validity between the two different estimates obtained from different sources.

The ROK is a relative comparison between the Total Benefits and Total Costs columns. The numbers in the ROK column can be used as the origin for determining which sub-processes are providing the least amount of value in the overall account management process. Low percentages represent low return and yield low value to NAVRES. It was decided to concentrate on these sub-processes and allocate the resources by deleting them, merging them, or increasing their value by decreasing their time to complete, thus making them more efficient.

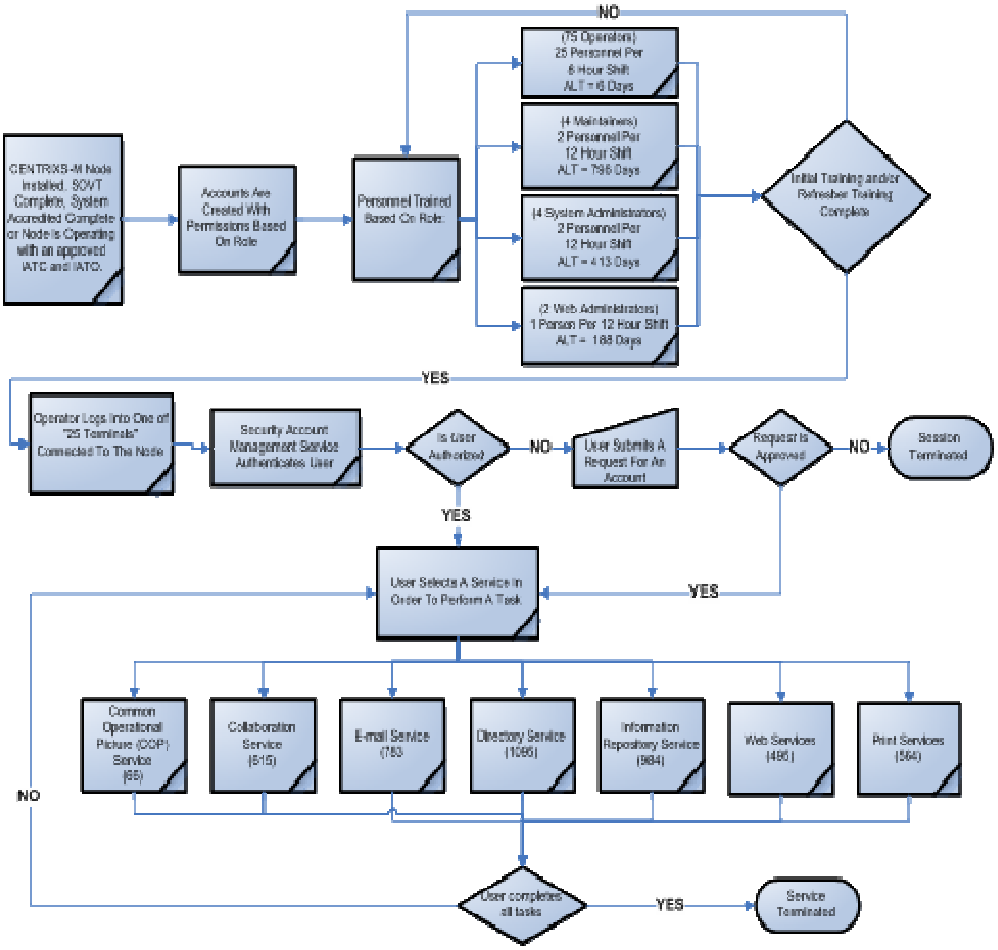
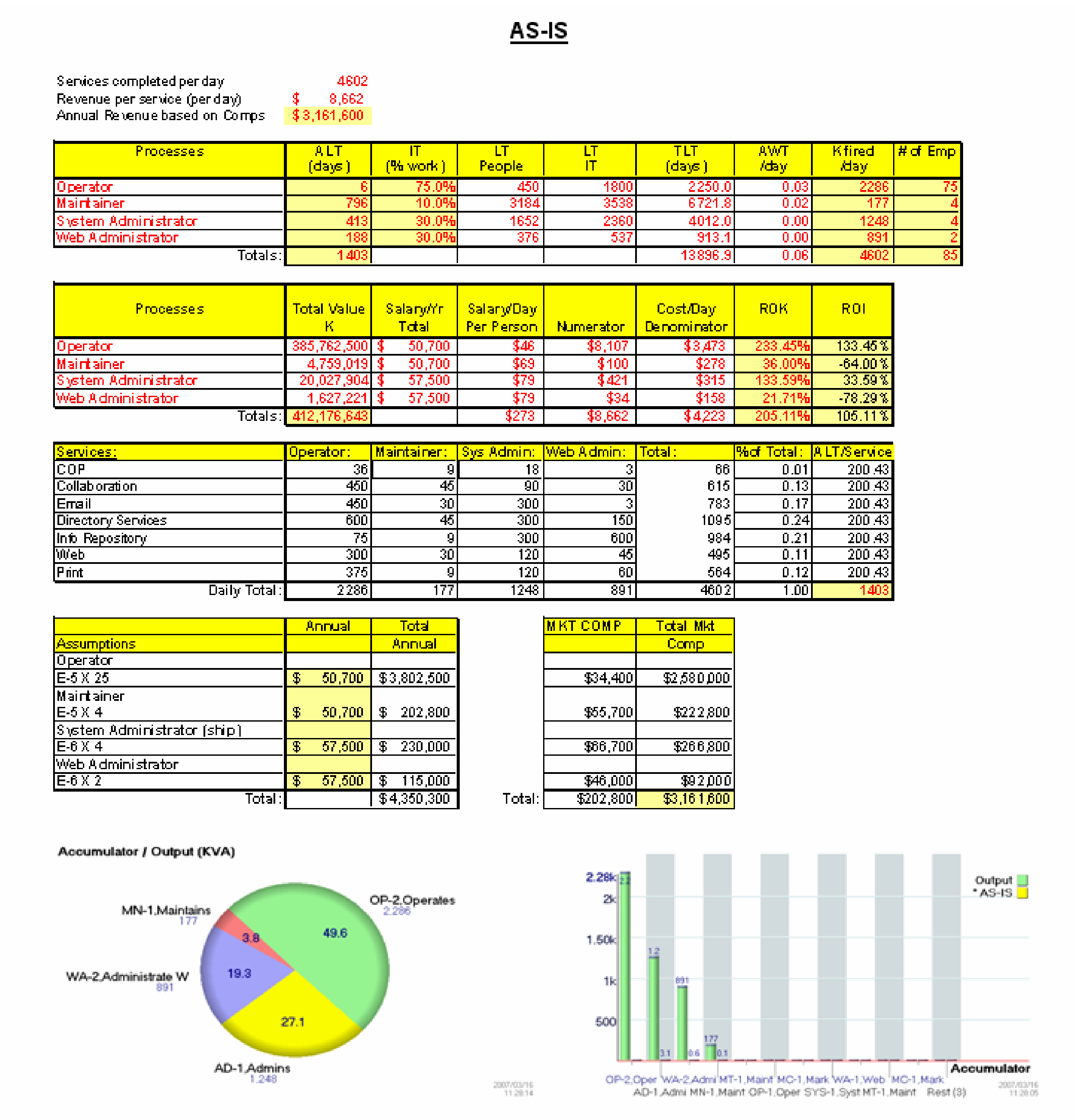

CENTRIXS -M Node Installed, SOVT Complete, System Accredited Complete or Node is Operating with an approved IATC and IATO.
Accounts Are Created With Permissions Based On Role
Personnel Trained Based On Role:
NO
(75 Operators) 25 Personnel Per 6 Hour Shift ALT = 6 Days
(4 Maintainers) 2 Personnel Per 12 Hour Shift ALT = 798 Days
(4 System Administrators) 2 Personnel Per 12 Hour Shift ALT = 4 13 Days
(2 Web Administrators) 1 Person Per 12 Hour Shift ALT = 188 Days
Initial Training and/or Refresher Training Complete
YES
Operator Logs Into One of "25 Terminals" Connected To The Node
Security Account Management Service Authenticates User
Is User Authorized
NO
User Submits A Request For An Account
Request Is Approved
NO
Session Terminated
YES
User Selects A Service In Order To Perform A Task
YES
Common Operational Picture (COP) Service (65)
Collaboration Service (615)
E-mail Service (783
Directory Service (1095)
Information Repository Service (984)
Web Services (495)
Print Services (564)
NO
User completes all tasks
YES
Service Terminated

Figure 10. “AS-IS” Process Flowchart



AS-IS

Services completed per day	4602
Revenue per service (per day)	$ 8,662
Annual Revenue based on Comps	$ 3,161,600

Processes	ALT (days)	IT (% work)	LT People	LT IT	TLT (days)	AWT /day	K fired /day	# of Emp
Operator	6	75.0%	450	1800	2250.0	0.03	2286	75
Maintainer	796	10.0%	3184	3538	6721.8	0.02	177	4
System Administrator	413	30.0%	1652	2360	4012.0	0.00	1248	4
Web Administrator	188	30.0%	376	537	913.1	0.00	891	2
Totals:	1403				13896.9	0.06	4602	85

Processes	Total Value K	Salary/Yr Total	Salary/Day Per Person	Numerator	Cost/Day Denominator	ROK	ROI
Operator	385,762,500	$ 50,700	$46	$8,107	$3,473	233.45%	133.45%
Maintainer	4,759,019	$ 50,700	$69	$100	$278	36.00%	-64.00%
System Administrator	20,027,904	$ 57,500	$79	$421	$315	133.59%	33.59%
Web Administrator	1,627,221	$ 57,500	$79	$34	$158	21.71%	-78.29%
Totals:	412,176,643		$273	$8,662	$4223	205.11%	105.11%

Services:	Operator:	Maintainer:	Sys Admin:	Web Admin:	Total:	% of Total:	ALT/Service
COP	36	9	18	3	66	0.01	200.43
Collaboration	450	45	90	30	615	0.13	200.43
Email	450	30	300	3	783	0.17	200.43
Directory Services	600	45	300	150	1095	0.24	200.43
Info Repository	75	9	300	600	984	0.21	200.43
Web	300	30	120	45	495	0.11	200.43
Print	375	9	120	60	564	0.12	200.43
Daily Total:	2286	177	1248	891	4602	1.00	1403

	Annual	Total		MKT COMP	Total Mkt
Assumptions		Annual			Comp
Operator					
E-5 X 25	$ 50,700	$3,802,500		$34,400	$2,580,000
Maintainer E-5 X 4	$ 50,700	$ 202,800		$55,700	$222,800
System Administrator (ship)					
E-6 X 4	$ 57,500	$ 230,000		$66,700	$266,800
Web Administrator					
E-6 X 2	$ 57,500	$ 115,000		$46,000	$92,000
Total:		$4,350,300	Total:	$202,800	$3,161,600

Figure 11. “AS-IS” KVA Spreadsheet with graphs generated in Radial Viewer

E. “AS-IS” SUMMARY

The quantitative calculation of ROK is the Total Benefits (the numerator) divided by the Total Cost (the denominator.) The numerator (Total Benefits) is the total learning time, which is derived from the ALT multiplied by the number of times the learning is fired (number of units/services involved, times the number of people involved in each of the sub-processes.)

The denominator (Total Costs per day) is the time it takes to complete the cumulative number of services from all sub-processes, per day, multiplied by the number of people involved per unit, multiplied by the times fired (number of times one person performs each sub-process per week and per hour). The percentage of IT was factored into the learning of each of the roles since basically all of the services were the same level of complexity. The IT percentage for Operators was determined to be as follows: 45%, Maintainers 10%, System Administrators 30%, and Web Administrators 30%. In analyzing the "AS-IS" process, we concluded that the issue was not the lack of IT, but rather the lack of integration or multi-tasking by the operators at each of the 25 terminals. The results of the "AS-IS" analysis made it possible to develop the proposed "To-Be" solution in order to comply with the mandatory 30 percent in Operator manning, which we imposed on the process to improve efficiency. The "AS-IS" Process yields a Total K = 243,843,916, ROK = 205.11% and ROI = 105.11%

F. THE PROPOSED "TO-BE" SOLUTION

The "To-Be" prototype was developed in response to the mandatory 30 percent reduction in operator manning. This prototype is a recommendation and has neither been tested, nor is it fully functional. Therefore, the "To-Be" solution is strictly for analyzing the impact of enforcing the mandatory reduction in operators by 30 percent. The assumptions, which were made when designing the "To-Be" prototype, are as follows:

- The purpose of the prototype is to comply with a 30 percent reduction in operator manning vice an attempt to maximize KVA and/or ROI.
- Each CENTRIXS node will continue to average 25 terminals per installation regardless of how the network is manned.
- Operator manning will be reduced from 25 to 17 per eight hour shift.
- Operators work an eight-hour shift, while maintainers, system administrators, and web administrators work 12-hour shifts.

- System administrator manning will be reduced from four to two (one person per shift.)
- Market comparables are based on the Government Service (GS) pay scale for equivalent employees based on role. The following determinations were made: maintainers = GS=5, system administrators = GS-12, and web administrators = GS-9.

The percentage of embedded IT varies based on role. Based on conversations with PMW-160 representatives, the following determination was made for embedded IT in order to maximize efficiency: IT for operators = 75 percent, maintainers = 10 percent, system administrators = 30% and web administrators = 30 percent.

G. "TO-BE" SUMMARY

The "To-Be" process flowchart and KVA spreadsheet were created in response to our self-imposed mandatory 30 percent reduction in CENTRIXS operator manning. The "To-Be" Process Flowchart (Figure 12) illustrates the processes, which were either changed, or eliminated to comply with the mandatory reduction in operators. Both the "To-Be" flowchart, and KVA spreadsheet (Figures 12 and 13) reflect a decrease in the total number of terminal operators from 75 to 51 per day, which reduces the number of operators per shift from 25 to 17. In addition, we reduced the number of System Administrators by 50 percent from 4 to 2. This mandatory reduction in operators is achievable through using split screens and empowering personnel to multi-task. Since the average time for firing knowledge is approximately 20 minutes, operators have ample time to both monitor and perform more that one service at a time. Our assumption regarding the knowledge embedded in the IT systems is that the IT embedded knowledge will remain the same.

However, as future IT systems are implemented, which require less operator knowledge, it is highly probable there will be a further merging of processes. The "To-Be" KVA spreadsheet represents the relative comparison between the ROK for the "AS-IS" and the "To-Be" processes. A relative comparison between the two yields a 30 percent operator manning reduction which increases ROK from 205.11% to 301.97%. In addition, the ROI increased from 105.11% to 201.97%. The "To-Be" process yields a

Total K = 251,137,555, ROK = 301.97% and ROI = 201.97%. The denominator for the "To-Be" process (Cost per day) also decreased from $3,473 to $2,361, which is a significant savings.

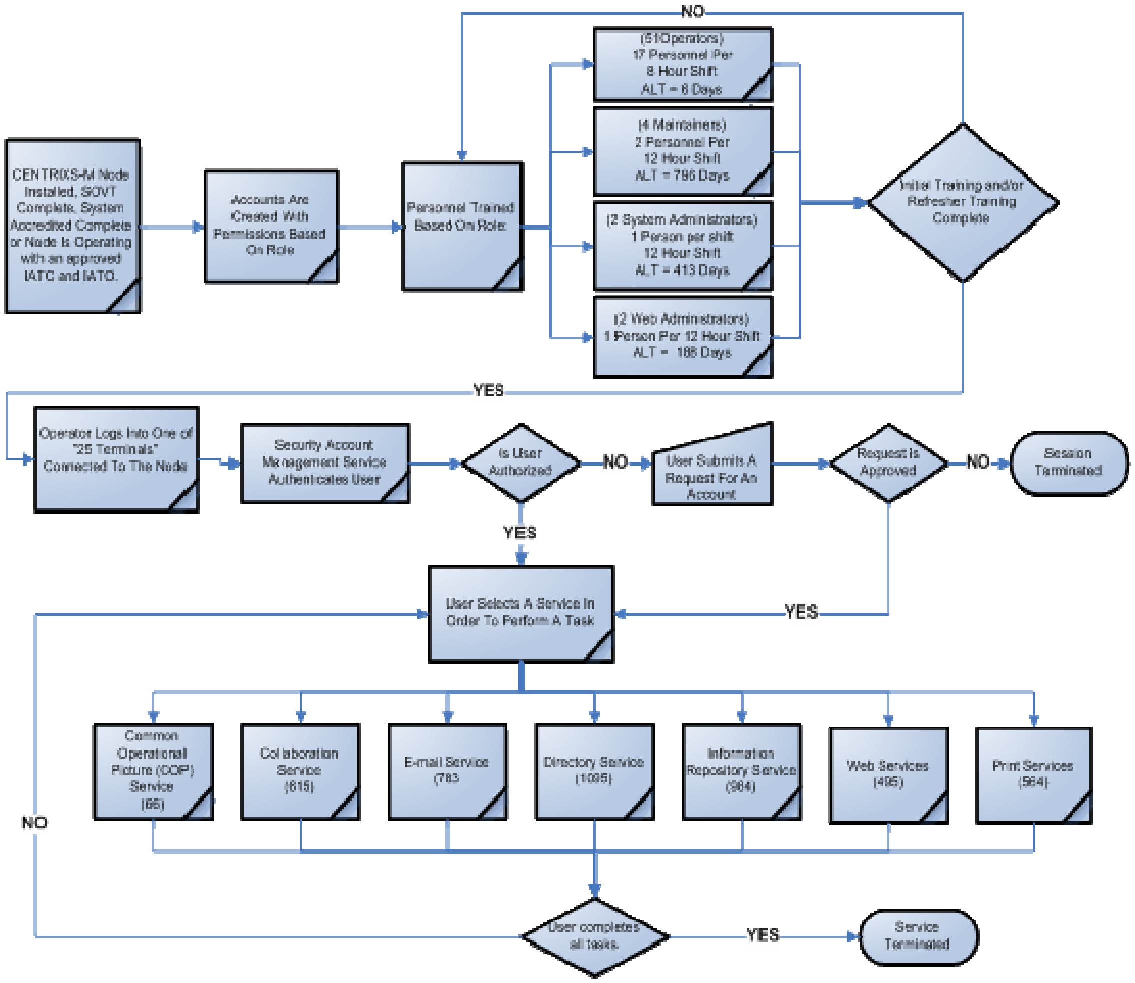
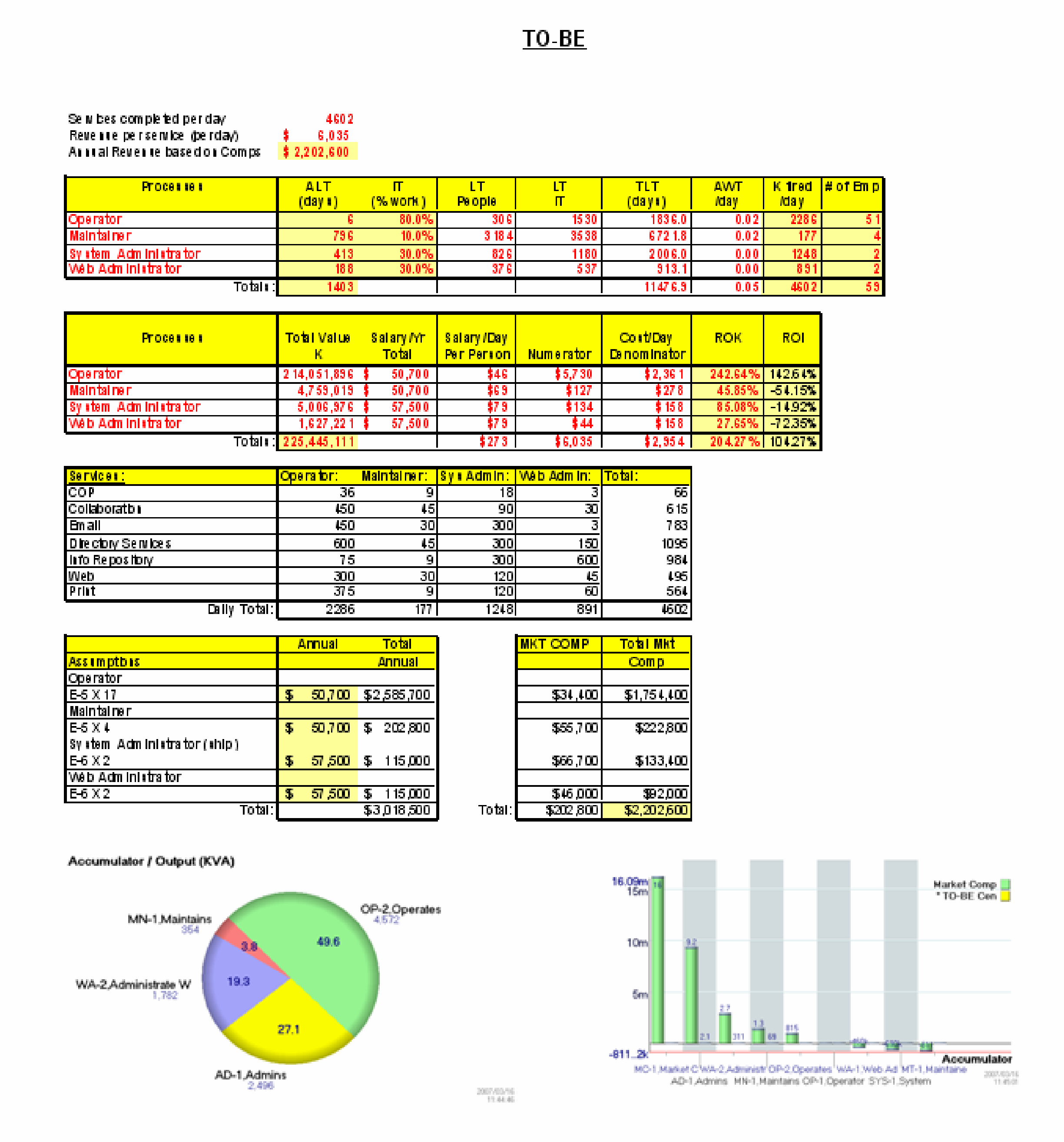

CENTRIXS-M Node Installed, SOVT Complete, System Accredited Complete or Node Is Operating with an approved IATC and IATO.
Accounts Are Created With Permissions Based On Role
Personnel Trained Based On Role
NO
(51 Operators) 17 Personnel Per 8 Hour Shift ALT = 6 Days
(4 Maintainers) 2 Personnel Per 12 Hour Shift ALT = 796 Days
(2 System Administrators) 1 Person per shift 12 Hour Shift ALT = 413 Days
(2 Web Administrators) 1 Person Per 12 Hour Shift ALT = 186 Days
Initial Training and/or Refresher Training Complete
YES
Operator Logs Into One of "25 Terminals" Connected To The Node
Security Account Management Service Authenticates User
Is User Authorized
NO
User Submits A Request For An Account
Request Is Approved
NO
Session Terminated
YES
User Selects A Service In Order To Perform A Task
YES
Common Operational Picture (COP) Service (65)
Collaboration Service (615)
E-mail Service (783
Directory Service (1035)
Information Repository Service (984)
Web Services (495)
Print Services (564)
NO
User completes all tasks.
YES
Service Terminated

Figure 12.   "To-Be" process flowchart.



TO-BE

Services completed per day	4602
Revenue per service (per day)	$ 6,035
Annual Revenue based on Comps	$ 2,202,600

Processes	ALT (days)	IT (% work)	LT People	LT IT	TLT (days)	AWT /day	K fired /day	# of Emp
Operator	6	80.0%	306	1530	1836.0	0.02	2286	51
Maintainer	796	10.0%	3184	3538	6721.8	0.02	177	4
System Administrator	413	30.0%	826	1180	2006.0	0.00	1248	2
Web Administrator	188	30.0%	376	537	913.1	0.00	891	2
Totals:	1403				11476.9	0.05	4602	59

Processes	Total Value K	Salary/Yr Total	Salary/Day Per Person	Numerator	Cost/Day Denominator	ROK	ROI
Operator	214,051,896	$ 50,700	$46	$5,730	$2,361	242.64%	142.64%
Maintainer	4,759,019	$ 50,700	$69	$127	$278	45.85%	-54.15%
System Administrator	5,006,976	$ 57,500	$79	$134	$158	85.08%	-14.92%
Web Administrator	1,627,221	$ 57,500	$79	$44	$158	27.65%	-72.35%
Totals:	225,445,111		$273	$6,035	$2,954	204.27%	104.27%

Services:	Operator:	Maintainer:	Sys Admin:	Web Admin:	Total:
COP	36	9	18	3	66
Collaboration	450	45	90	30	615
Email	450	30	300	3	783
Directory Services	600	45	300	150	1095
Info Repository	75	9	300	600	984
Web	300	30	120	45	495
Print	375	9	120	60	564
Daily Total:	2286	177	1248	891	4602

	Annual	Total
Assumptions		Annual
Operator		
E-5 X 17	$ 50,700	$2,585,700
Maintainer		
E-5 X 4	$ 50,700	$ 202,800
System Administrator (ship)		
E-6 X 2	$ 57,500	$ 115,000
Web Administrator		
E-6 X 2	$ 57,500	$ 115,000
Total:		$3,018,500

MKT COMP	Total Mkt
	Comp
$34,400	$1,754,400
$55,700	$222,800
$66,700	$133,400
$46,000	$92,000
Total: $202,800	$2,202,600

Figure 13. “To-Be” KVA Spreadsheet with graphs generated in Radial Viewer

H. THE PROPOSED “RADICAL” SOLUTION

The “Radical” prototype was an attempt to aggressively pursue the intent of the “To-Be” mandatory 30 percent reduction in operator manning. This prototype is a recommendation and is neither tested, nor fully functional. As with the “To-Be” prototype, the “Radical” prototype is strictly a tool for analyzing the impact of making further manpower reductions, while maintaining the same performance demonstrated in the “AS-IS” process. The “Radical” process demonstrates the impact of implementing a 68% reduction in operators and a 100% reduction in web administrators as depicted in Figures 14 and 15. Total manning reduction reduces manning from 85 personnel to 32, which translates to a 62% reduction in manning. The assumptions, which were made when designing the “Radical” prototype are as follows:

- The purpose of the prototype is an attempt to maximize the intent of the mandatory 30% reduction in operator manning, which will basically determine the minimal manning required for a CENTRIXS node.
- Each CENTRIXS node will continue to average 25 terminals per installation regardless of how the network is manned.
- Operators receive an additional 30 days of training (36 days total) in order to teach them multi-tasking and how to efficiently monitor more than one terminal.
- Operator manning is reduced from 75 personnel to 24, with eight operators each manning three terminals through the use of A/B/C Switches and some additional training.
- Operators still work an eight hour shift, while maintainers and system administrators work 12 hour shifts.
- The role of web administrators was severely under utilized, and therefore system administrators will absorb the duties and responsibilities of the web administrators.
- Market comparables and embedded IT were calculated in the same manner as the “To-Be” process and are described under the “To-Be” proposed solution.

The “Radical” process yielded a Total K = 281,126,494, ROK = 586.01% and ROI = 486.01% with a Total cost per day = $1,111.

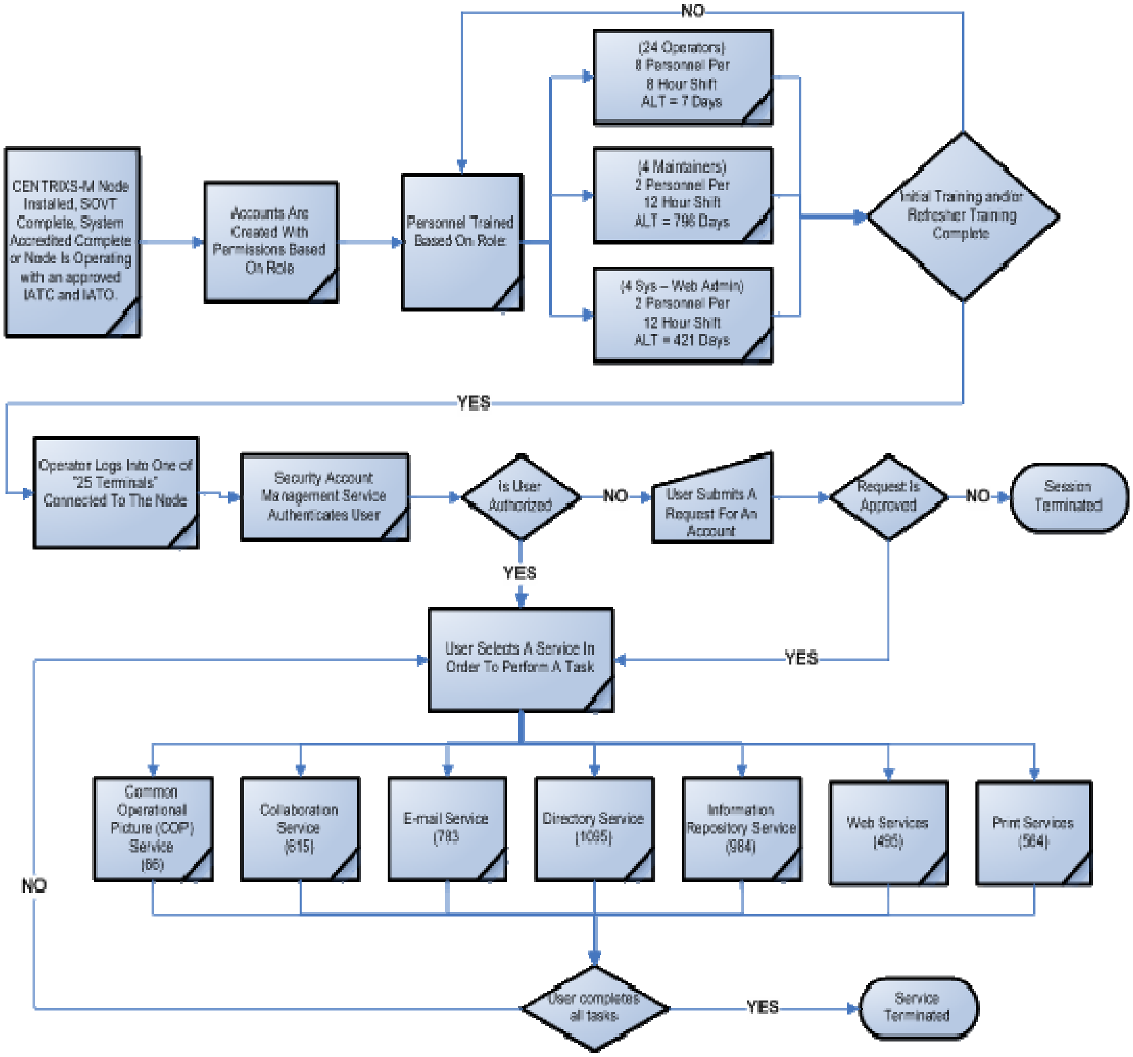
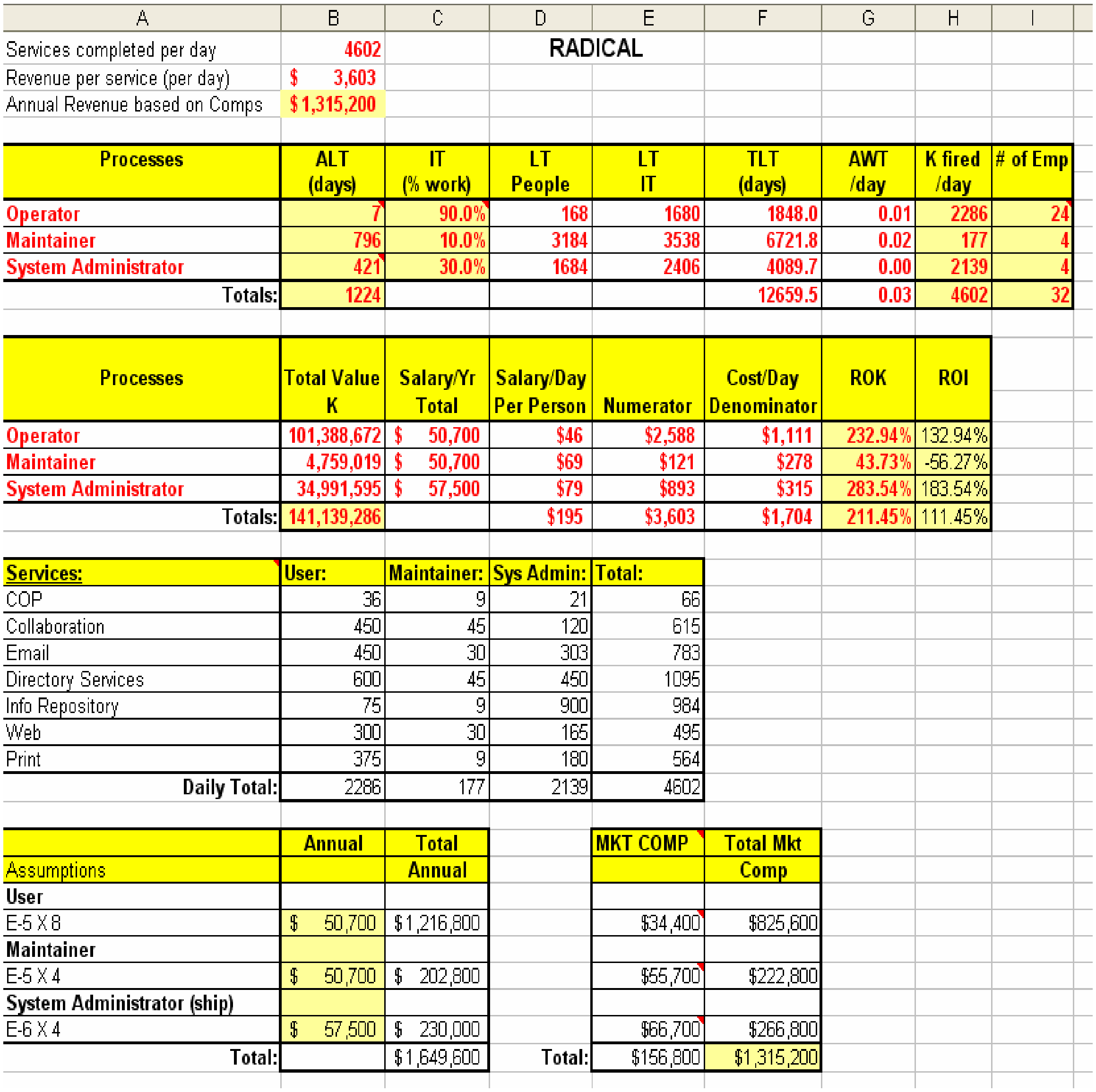

CENTRIXS-M Node Installed, SOVT Complete, System Accredited Complete or Node Is Operating with an approved IATC and IATO.
Accounts Are Created With Permissions Based On Role
Personnel Trained Based On Role
NO
(24 Operators) 8 Personnel Per 8 Hour Shift ALT = 7 Days
(4 Maintainers) 2 Personnel Per 12 Hour Shift ALT = 798 Days
(4 Sys – Web Admin) 2 Personnel Per 12 Hour Shift ALT = 421 Days
Initial Training and/or Refresher Training Complete
YES
Operator Logs Into One of "25 Terminals" Connected To The Node
Security Account Management Service Authenticates User
Is User Authorized
NO
User Submits A Request For An Account
Request Is Approved
NO
Session Terminated
YES
User Selects A Service In Order To Perform A Task
YES
Common Operational Picture (COP) Service (66)
Collaboration Service (615)
E-mail Service (783
Directory Service (1095)
Information Repository Service (984)
Web Services (495)
Print Services (564)
NO
User completes all tasks
YES
Service Terminated

Figure 14. “Radical” Process Flowchart



	A	B	C	D	E
	Services completed per day	4602		RADICAL	
	Revenue per service (per day)	$ 3,603			
	Annual Revenue based on Comps	$1,315,200			

Processes	ALT (days)	IT (% work)	LT People	LT IT	TLT (days)	AWT /day	K fired /day	# of Emp
Operator	7	90.0%	168	1680	1848.0	0.01	2286	24
Maintainer	796	10.0%	3184	3538	6721.8	0.02	177	4
System Administrator	421	30.0%	1684	2406	4089.7	0.00	2139	4
Totals:	1224				12659.5	0.03	4602	32

Processes	Total Value K	Salary/Yr Total	Salary/Day Per Person	Numerator	Cost/Day Denominator	ROK	ROI
Operator	101,388,672	$ 50,700	$46	$2,588	$1,111	232.94%	132.94%
Maintainer	4,759,019	$ 50,700	$69	$121	$278	43.73%	-56.27%
System Administrator	34,991,595	$ 57,500	$79	$893	$315	283.54%	183.54%
Totals:	141,139,286		$195	$3,603	$1,704	211.45%	111.45%

Services:	User:	Maintainer:	Sys Admin:	Total:
COP	36	9	21	66
Collaboration	450	45	120	615
Email	450	30	303	783
Directory Services	600	45	450	1095
Info Repository	75	9	900	984
Web	300	30	165	495
Print	375	9	180	564
Daily Total:	2286	177	2139	4602

	Annual	Total		MKT COMP	Total Mkt
Assumptions		Annual			Comp
User					
E-5 X 8	$ 50,700	$1,216,800		$34,400	$825,600
Maintainer					
E-5 X 4	$ 50,700	$ 202,800		$55,700	$222,800
System Administrator (ship)					
E-6 X 4	$ 57,500	$ 230,000		$66,700	$266,800
Total:		$1,649,600	Total:	$156,800	$1,315,200

Figure 15. “Radical” KVA Spreadsheet

I. CONCLUSION

The CENTRIXS system will soon reach the Initial Operational Capability (IOC) and will become an official Program of Record. Therefore, as the technology becomes more mature and prevalent, Information Technology managers will need to understand the CENTRIXS architecture and how to communicate efficiently and effectively with our coalition partners. Hopefully, this thesis will be a stimulus to look closer at how we are manning CENTRIXS nodes and the associated terminals. One key assumption with this portion of our thesis is that the complexity of all sub-processes is equal, and therefore the percentage of training time is proportional across all seven sub-processes. The “AS-IS”, “To-Be”, and “Radical” process flowcharts, as well as the KVA spreadsheets clearly show that we can reduce total cost per day, while also increasing Total Return, Return on Knowledge, and Return on Investment.

The operators are an important part of the process and generate the bulk of the daily services provided by CENTRIXS. Therefore, operators, if given the opportunity, have the ability to make useful recommendations for changes and improvements in the process. One way operators can contribute would be through creating a forum or Community of Interest (COI), where operators could express their concerns and make recommendations. Working groups and training teams would also be valid methods of collecting and analyzing recommendations for improvement. These working groups could be established based on role, which would enable operators, maintainers, and administrators to collaborate on ways to improve the process.

Another recommendation is to include the requisite CENTRIXS training in the core training pipeline for enlisted personnel (ET/IT/IS/OS) who fill the required roles. Since virtually all platforms will eventually have CENTRIXS nodes, it makes sense to include the apprentice or “A” School level of training. Bringing CENTRIXS to the school house vice mobile training teams would create the opportunity to develop the active duty CENTRIXS instructors into resident experts on the system.

Even though all ships do not yet have CENTRIXS installed on a permanent basis, ships are equipped with CENTRIXS when they deploy. Therefore, as CENTRIXS becomes ubiquitous, it is critical the Navy increase the baseline knowledge level throughout the fleet. Currently, many actors are functional after the training, but not fully aware of all the resources available at their finger tips. One in particular, is the use of Microsoft® Active Directory, vice using the Global Address List (GAL) to verify existing accounts. The majority of CENTRIXS operators are unaware of how to map their local computer using Active Directory in order to view exactly which accounts are being utilized. Instead, operators use email profile information from the GAL. It is understood that the actors want to manage properly, but they do not know how to manage because they have not been properly trained. This could easily be resolved through something as simple as a web-based curriculum, which would focus on how to use the currently available tools as well as best practices. Education and training in this area is critical, and if not pursued will continue to have a negative impact on CENTRIXS operations. Future initiatives could also include incorporation of courses on Navy Knowledge Online (NKO) or the schoolhouse at the "A" and "C" school level.

Lastly, the other recommendation made in the "Radical" process, which should be considered and researched, is making the system push vice pull. Operators would then be able to spend more time managing information vice seeking it. In addition, improvements in technology will eventually merge more and more existing technology and systems enabling us to do more with less. However, until those technologies are fielded and tested, we need to resist the urge to reduce our manning before the technology matures. By determining the current "AS-IS", "To-Be", and "Radical" processes as well as using KVA, we were able to measure the knowledge in each of the sub-processes. This thesis will assist future CENTRIXS managers with identifying which roles and sub-processes are not providing value to the overall process so they can make logical decisions and recommends. The following pages are diagrams designed to paint a picture of connectivity and organization of CENTRIXS networks. Appendix F includes an Operational Activity Model overview, which is used to clearly delineate lines of responsibility, uncover unnecessary operational activity redundancy, make decisions about streamlining, combining, or omitting activities, and define or flag issues, opportunities, or operational activities and their interfaces (information flows among the activities) that need to be scrutinized further. The Operational Activity Model graphically illustrates the "how" (operational activities) and "what" (Information Exchanges) data elements of a given architecture at the owner's level of detail.

IV. ACQUISITION, INSTALLATION, AND ACCREDITATION

A. INTRODUCTION

The Integrated Defense Acquisition, Technology and Logistics (IADT&L) Life Cycle Management Framework is comprised of three major Decision Support Systems (DSS). The first DSS, the Defense Acquisition System (DAS) is the management process by which the Department of Defense (DoD) provides effective, affordable, and timely systems to the users (DoDD 5000.1 and DoDI 5000.2). DAS is the Acquisition Management piece and exists to manage the Nation's investments in technologies, programs, and product support necessary to achieve the National Security Strategy and support the U.S. Armed Forces. The second DSS, the Joint Capabilities Integration and Development System (JCIDS) is the Capabilities Development piece. JCIDS establishes procedures for supporting both the Chairman of the Joint Chiefs of Staff (CJCS) and the JROC in identifying, assessing, and prioritizing joint military capability needs (CJCSI 3170.01E). JCIDS implements a capabilities-based approach which effectively leverages the expertise of all government agencies, industry, and academia to identify improvements to existing capabilities and to develop new war-fighting capabilities. The third DSS, the Planning, Programming, Budget, and Execution (PPBE), is the resource allocation process and is controlled by the Secretary of Defense (DoD 7045.14 / MID-913). The PPBE DSS is used to establish, maintain, and revise the Future Years Defense Plan and to execute the DoD budget. This approach requires a collaborative process, which uses joint concepts and integrated architectures to identify prioritized capability gaps and synchronize Doctrine, Organization, Training, Material (Technology), Leadership and Education, Personnel (Culture) and Facilities (DOTMLPF) in order to resolve those gaps.

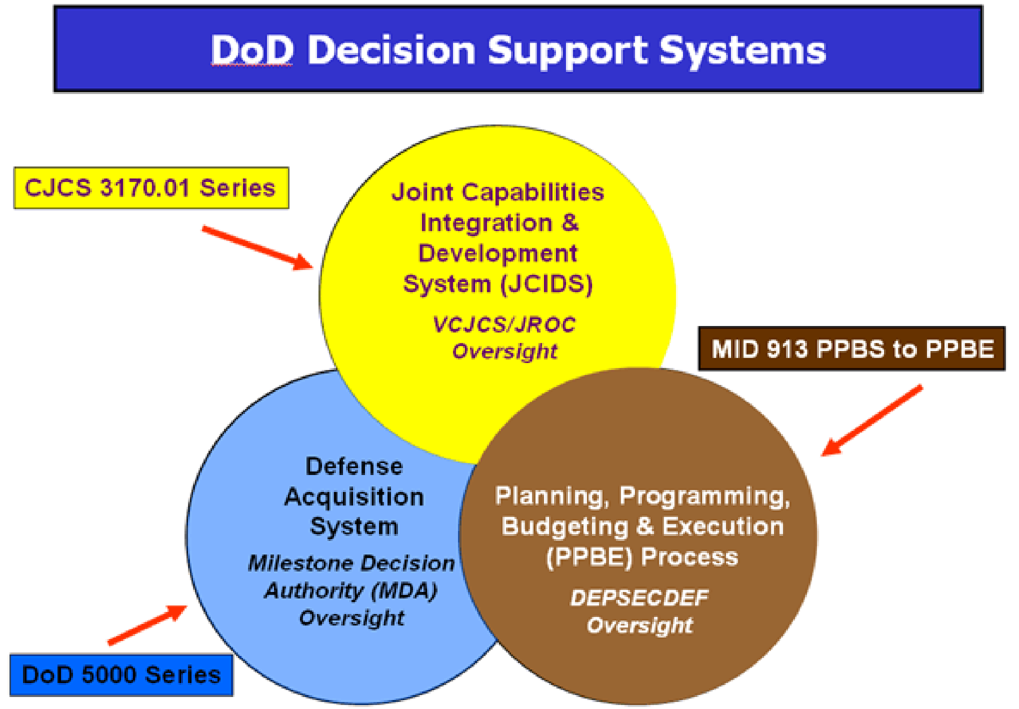

DoD Decision Support Systems
CJCS 3170.01 Series
Joint Capabilities Integration & Development System (JCIDS)
VCJCS/JROC Oversight
MID 913 PPBS to PPBE
Defense Acquisition System
Milestone Decision Authority (MDA) Oversight
Planning, Programming, Budgeting & Execution (PPBE) Process
DEPSECDEF Oversight
DoD 5000 Series

Figure 16. DoD Decision Support Systems (DSS) (From: Cochrane, 5, 2004)

The acquisition process is structured into discrete phases, which are separated by milestones or major decision points. These milestones in conjunction with key activities enable comprehensive management of the process and provide informed decision making. The acquisition process begins with identifying a capability need, which requires a material solution. There are five categories of policies and principles that govern the DAS, which are discussed in detail in DoD 5000.1:1 and illustrated in Figure 17. The typical approach is for the DoD components is to first try to meet new capability needs through non-material solutions. However, if existing systems or on-hand material cannot be used or modified in an economic manner then a material solution is sought out. Each defense acquisition program is assigned a Program Manager (PM) who is responsible for the Acquisition Management Framework and meeting the war fighter's needs.

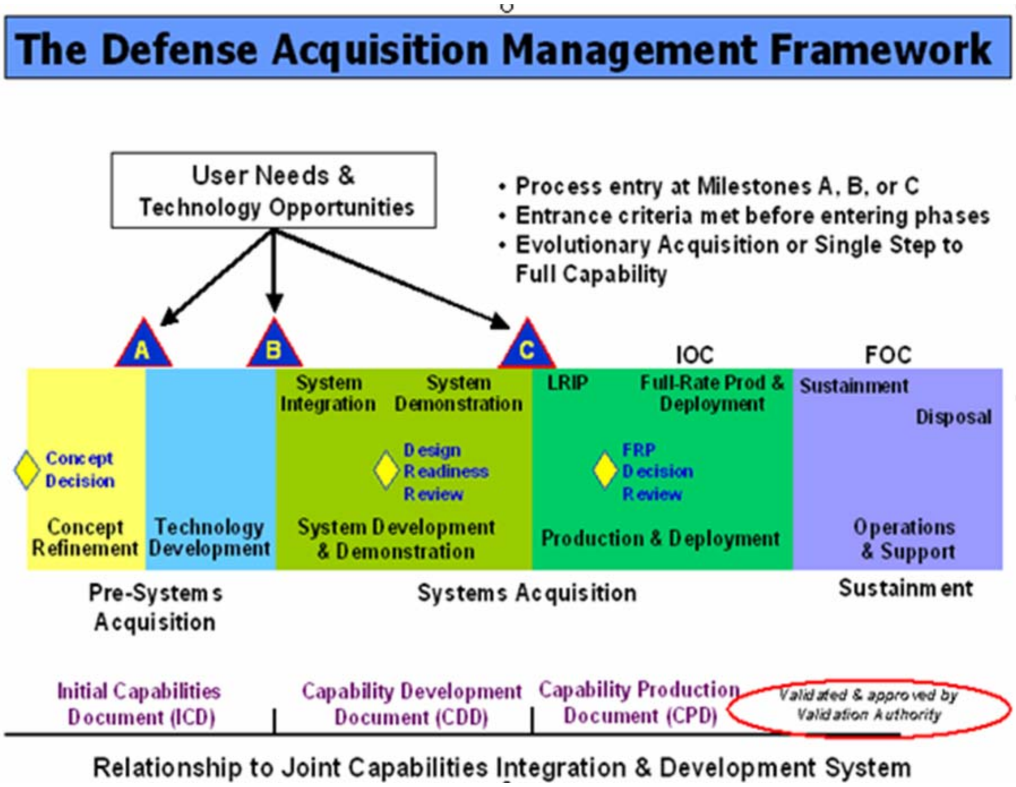

The Defense Acquisition Management Framework
User Needs & Technology Opportunities
• Process entry at Milestones A, B, or C
• Entrance criteria met before entering phases
• Evolutionary Acquisition or Single Step to Full Capability
A
B
C
IOC
FOC
System Integration
System Demonstration
LRIP
Full-Rate Prod & Deployment
Sustainment
Disposal
Concept Decision
Design Readiness Review
FRP Decision Review
Concept Refinement
Technology Development
System Development & Demonstration
Production & Deployment
Operations & Support
Pre-Systems Acquisition
Systems Acquisition
Sustainment
Initial Capabilities Document (ICD)
Capability Development Document (CDD)
Capability Production Document (CPD)
Validated & approved by Validation Authority
Relationship to Joint Capabilities Integration & Development System

Figure 17. Defense Acquisition Management Framework, Milestones, and JCIDS relationship (From: Cochrane, 3, 2005)

The PM bears sole accountability and responsibility for accomplishing the objectives for Total Life Cycle Systems Management, which also includes sustainment and even disposal of the system. The PM is responsible for the entire system from design to disposal (cradle to grave) and the PM credo is to stay on Schedule, under Cost while meeting or exceeding Performance specifications (Schedule, Cost and Performance).

JCIDS replaced the Requirements Generation System (RGS) in 2003 and the new JCIDS system requires several key documents be sequentially completed which support the milestones decisions. JCIDS Analysis begins with a Functional Area Analysis (FAA) to identify operational tasks, conditions and standards to achieve the program objectives. A Functional Needs Analysis (FNA) is then performed to determine capability gaps and if existing and programs which are already scheduled will be able to cover the gap in capability. Then a Functional Solution Analysis (FSA) explores the possibility of an integrated DOTMLPF solution and finally a Post Independent Analysis (PIA) is conducted which is an independent analysis, to determine the best fit. The end result of the completion of these steps is the Initial Capability Document (ICD) (CJCSI 3170.01F, 1-5, 2007.)

The ICD is the first of four documents, which provide inputs to the Knowledge Management Decision Support (DS) Tool. The ICD supports the JCIDS analysis concept decision and Milestone A and accomplishes this by describing why a material approach is needed to solve a capability gap. The ICD summarizes the analysis of the DOTMLPF process and documents why other non-material solutions are inadequate to fulfill the gap in capability. The second document, the Capability Development Document (CDD) supports program initiation at Milestone B by describing the evolutionary acquisition strategy, which will be used for the program. The acquisition strategy depends on how well the requirements are known, the technical maturity, complexity as well as many other factors. The CDD also describes and outlines the acceptable technical maturity, CMM as well as program logistics. The third document, the CPD supports Milestone C and addresses the production considerations for a single increment of a program. The fourth document, the Capstone Requirements Document (CRD) provides a common framework for further developing the CDDs and CPDs. CRDs will eventually be replaced by the joint war fighting functional capability Integrated Architectures. The ICD, CDD and CPD all feed the Knowledge Management (KM) DS tool (KMDS), which serves as a virtual library for review, approval and reference (DAU Press, 10, 2005.)

The KMDS repository feeds the JPD decision, which then branches into three different process flows depending on the significance of the program to joint war fighting. For ACAT I/IA/II programs where capabilities have significant impact on Joint War fighting there is JROC interest and review before the J2, J-4, J-6 review. For ACAT I/IA/II programs without significant joint war fighting impact there is Joint Integration before the J-2, J-4, J-6 review. For all other programs there is independent interest are reviews before the sponsor validates or approves the program. Both the JROC and Joint Integration provide input to the J-2, J-4 and J-6 for review before the Functional Capability Board (FCB) review. The FCBs act as action agents in order to lead the review of Service proposed functional needs analysis to ensure compliance with the series of JCIDS documents and to make recommendations to both the Joint Capabilities Board (JCB) and the JROC. Independent reviews provide inputs to the sponsor for validation and approval before it is submitted to the JCB and JROC for validation and approval (Cochrane, 28, 2005.) A graphic of the detailed JCIDS Data Flow is illustrated in Figure 18.

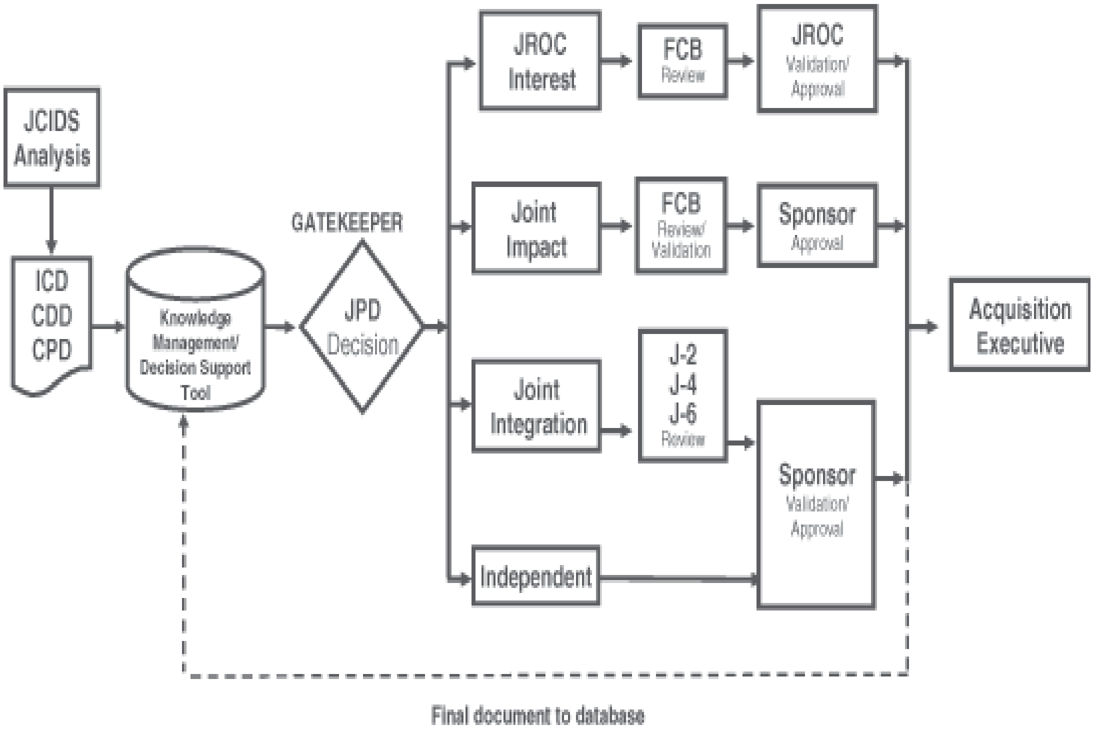


Figure 18. Detailed JCIDS Data Flow (From: Cochrane, 45, 2005)

The Network Centric FCB (NC FCB) is responsible for the organization, analysis, and prioritization of joint war fighting capabilities and has four primary responsibilities: The first function is to oversee a portfolio of network centric capabilities within JCIDS, DAS and PPBE. The second function is to lead in the development of network centric-related concepts, operational views of integrated architectures, as well as related studies to use the portfolio of network centric products as a framework for performing network centric capability analyses in support of JCIDS. The third responsibility of the NC FCB is to ensure horizontal integration of the network centric products across the other NC FCB functional areas. The fourth and final responsibility is to ensure both vertical and horizontal integration of communications capabilities across national, strategic, operational and tactical levels. The NC FCB also oversees the development and maintenance of network centric-related functional and integrating concepts and integrated architectures for JROC approval. Further, the NC FCB ensures the network-centric product lines include capabilities, attributes, measures and metrics. The NC FCB also coordinates both the integration and de-conflicts capability proposals relating to network-centric operations (CJCSI 3170.01F, 4, 2007.)

The Military Communications-Electronic Board (MCEB) addresses military communications-electronics issues referred by the Secretary of Defense (SECDEF), CJCS, DoD CIO, Military Departments (MILDEPs) as well as the heads of other DoD Components. The Joint Staff/J-6 is the Chairman of the MCEB and board membership is composed of representatives from each Service, U.S. Coast Guard, DISA, Defense Intelligence Agency (DIA), NSA, and the Vice-Director of J-6, who represents the COCOMs. The Assistant Secretary of Defense (NII) is the only non-chartered member invited to attend the executive session. The MCEB is the senior resolution, coordination, and prioritization body for matters related to NSS communications and interoperability testing issues within the war fighting enterprise mission area. The MCEB Chairman is mandated to inform the DoD CIO of all MCEB related matters, which may impact the DoD CIO responsibilities (MCBE, 27, 2002.)

The Joint Battle Management C2 (JBMC2) Board of Directors (JBMC2 BOD) was established by the USJFCOM under Management Initiative Decision 912 (MID 912) which was designed to strengthen the DoD ability to organize, train, and equip joint forces and to provide “system-of-systems” capabilities to the joint force. The JBMC2 BOD consists of G/FO or Senior Executive Service members from COCOMs, Services, and the Joint Staff (represented by a G/FO from J-6.) Optional advisory members consist of representatives from ASD (NII), OSD (AT&L), USD (I), Service and/or agency program sponsors and/or executive agents, and selected Defense agencies and the U.S. Coast Guard. The interface between the JBMC2 BOD and the JROC will occur via the JCIDS process (CJCSI 3170.01E.) When required, the JBMC2 BOD provides enter level recommendations to the JROC via the JCIDS process (i.e., Gatekeeper, JCB, or JROC.) The JROC ensures USJFCOM’s JBMC2 mission, capability area requirements, and system-of-systems capability requirements are synchronized with other mission areas.

The JROC will also ensure Service and agency JBMC2 efforts are aligned, integrated, and coordinated with the USJFCOM integrated architectures and requirements (JCS, 88, 2006.)

There is also a requirement to both tightly link and manage defense department software components as part of the overall systems engineering process. There are numerous software specific considerations and specifications which must be adhered to within the DoD. Two DoD standards for software specifications are DoD Standard Data (DoD 8320.1) and DoD Net-Centric Data Strategy. Additionally the IA considerations and specifications are covered by the DoD IT Security Certification and Accreditation Process (DITSCAP) throughout a programs life cycle. For IT systems programs the details of the enterprise and domain architecture are instrumental to ensuring the programs are scalable and interoperable. FORCENET serves as the overall enterprise architecture for CENTRIXS-M and the DoD Architecture Framework (DoDAF) requires that specific operational, systems and technical views be produced during the programs life cycle. The Clinger-Cohen Act (CCA) also applies to all federal IT and National Security Systems (NSS) acquisitions. The DAU 5000 series processes are inherently CCA compliant and formal certifications by milestones are required. Further, in accordance with (IAW) Public Law 108-87 all programs are required to provide formal compliance notification to Congress and PMs are required to report key parameters for their programs online using the DoD IT Registry (Cochrane, 23, 2003.)

The IDATL process includes three technical management plans with the Systems Engineering Plan (SEP) being the only mandatory plan required for each milestone. The Integrated Master Plan (IMP) is an optional even driven plan used to manage a programs major tasks and activities. The Integrated Master Schedule (IMS) is also optional and often integrated with the IMP to display how work efforts relate to tasks and activities. The command structure is also important to the program and needs to support the IDATL process (IDATL, 6, 2005.)

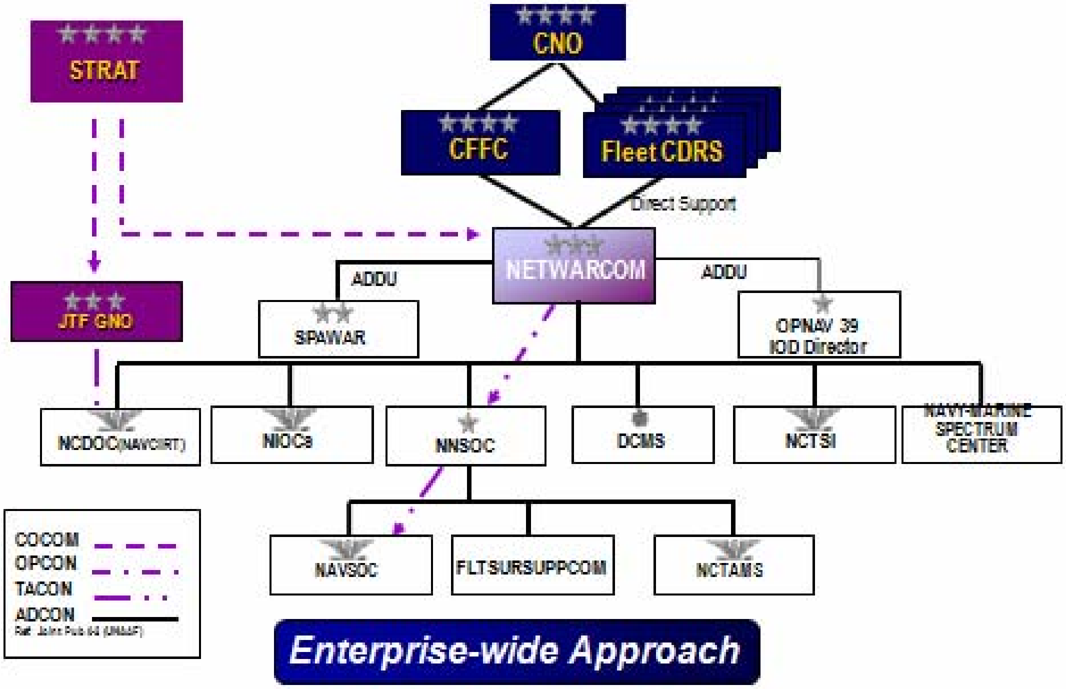


Figure 19. FORCENET and CENTRIXS Enterprise (From: Fetter, 36, 2006)

B. CENTRIXS ACQUISITION

In November 1999, Senior Defense Leadership formed the Interoperability Senior Steering Group (ISSG) as one of the Defense Intelligence Agency’s (DIA) four focus areas. Leadership appointed U.S. Central Command (USCENTCOM) as the lead for the ISSG’s efforts that included developing a similar CENTRIXS system. USCENTCOM Theater Engagement Plan (TEP) 1999-2003 established the requirement for a MNIS. In response, the USCENTCOM Cooperative Defense Initiative (CDI) Campaign Plan 00-01 and the USCENTCOM Coalition C4I Interoperability Plan March 2001, further defined the goal coalition network as providing “an integrated, interoperable, multidiscipline C4I/Shared Early Warning (SEW) System-of-Systems (SoS)” for U.S. and Gulf Cooperation Council (GCC) nations, plus Egypt and Jordan (GCC+2) decisions makers.

The terrorist attacks of September 11, 2001, motivated USCENTCOM to pursue OEF and efforts focused on rapidly developing and implementing a network intelligence interoperability solution to support warfighting operations. Overarching requirements included: CIP and COP sharing ISR and Coalition operations (Boardman, 24, 2004.)

With CENTRIXS firmly established as the DoD MNIS portion of the GIG, the Navy established CENTRIXS-Maritime (CENTRIXS-M) in 2004 as the maritime variant of CENTRIXS. CENTRIXS-M. CENTRIXS-M was initially fielded as a project in 2002 under the Coalition Wide Area Network (COWAN) which was funded under the Defense Emergency Response Fund (DERF), Office of the Secretary of Defense (OSD) and Fleet Operations and Maintenance (OMN). CENTRIXS-M absorbed COWAN-Lite in FY04 in order to create a single coherent Navy project and gained formal re-sourcing by OPNAV N6 in FY06. PMW-160 has established an Accelerated Acquisition Plan (AAP) for the sustainment of legacy CENTRIXS-M Block 0 I and II systems.

The capability of CENTRIXS-M to share data and information with coalition and allied forces both enhances and extends the GIG to the afloat war fighters. CENTRIXS-M aligns with FORCENET objectives of improved combat capability and knowledge-based combat operations, which increase, force survivability (Soriano, 2007.)

C. CENTRIXS STATUS

PMW-160 is the acquisition manager for the CENTRIXS shore NOC and shipboard system environments for the Navy. CENTRIXS Block II, Increment I (BLK II/I) became a PMW-160 POR in the first quarter of FY06 and is planned for Milestone C review by the MDA and Low Rate Initial Production (LRIP) in the second Quarter of FY08. PWM-160 submitted the CPD to OPNAV in July 2006 for entry to the JCID process. CENTRIXS-M BLK II/I is scheduled for the third quarter Milestone C is planned for FY08 and the IOC is planned for the second quarter of FY09 will reach Full Operational Capability (FOC) in FY16. CENTRIXS BLK II/I uses Trusted Sun Solaris 8.x for combining multiple coalition enclaves and distributing data to Multi-Level Thin Client (MLTC) devices resulting in decreased hardware/footprint by no longer requiring separate clients and back end servers for each enclave. The next generation, CENTRIXS-M Block 2, Increment II, will provide a single Ultra Thin Client (UTC) workstation which will use virtualized domains to support multiple coalition COIs.

CENTRIXS program is projected to receive Acquisition Category (ACAT III) designation. The criteria for DoD ACAT III designation states the program does not meet criteria for ACAT II or above and less than a MAIS program and the decision authority is designated by the DoD CAE at the lowest level appropriate. In addition, the SECNAV ACAT criteria for IT systems programs, is the program does not meet the criteria for ACAT II or above, program costs/year = $15 million = $32 million in FY 2000 constant dollars or total program costs = $30 million = $126 million in FY 2000 constant dollars or total life-cycle costs = $378 million in FY 2000 constant dollars. The ACAT III Decision Authority is the Cognizant PEO, SYSCOM Commander, DRPM, or designated flag officer or senior executive service (SES) official, ASN (RD&A), or designee, for programs not assigned to a PEO, SYSCOM, or DRPM (SECNAVINST 5000.2C, 2004)

The CENTRIXS Resource Sponsor is OPNAV N6F3, the Requirements Officer is OPNAV N6F311, the PM is PEO C4I (PMW-160), the Deputy Program Manager is PMW-160A, the Afloat Networks Division Head is PMW-160.1, and the CENTRIXS Assistant Program Manager is PMW-160.13 (Soriano, 2007). The Navy is scheduled to turn over the program to DISA in FY08. The CENTRIXS CPD, Version 2.0, was prepared on October 17, 2006 in order to support the MDA’s decisions regarding Milestone C for CENTRIXS Increment 1. The CENTRIXS program has been designated a JROC Interest/Joint Integration/Independent program. The CENTRIXS Block 2, Increment I design provides simultaneous access to multiple enclaves using MLTC architecture in order to reduce the Space, Weight and Power (SWaP) requirements aboard Unit and Force Level platforms (Soriano, 2007.)

The CENTRIXS design complies with OSA and DISR guidance for flexibility and interoperability. CENTRIXS uses both COTS and GOTS and is primarily a Non-Developmental Item (NDI). CENTRIXS capabilities are developed and provided incrementally with increasing capabilities being implemented as new and improved COTS/GOTS products become available. Key components within the CENTRIXS architecture are on a 3-year software and 4-year hardware technical refresh cycle, and may be updated prior to the release of a following, next generation increments.

The plan is to continue incorporating the CDS capabilities in the CENTRIXS program and to support the transition to the future MNIS program. CENTRIXS BLK II/I design builds on the capabilities of the previous variants, as a "technology bridge" to start incorporating CDS capabilities. Each CENTRIXS increment will have a separate CPD detailing the incorporation of new requirements. Earlier versions of CENTRIXS, identified as Blocks 0, I and II, were fielded under the original CENTRIXS program. CENTRIXS is a COTS/GOTS, largely NDI program. CENTRIXS capabilities are developed and provided incrementally with increasing capabilities being implemented as new and improved COTS/GOTS products become available. Key components within the CENTRIXS architecture are on a 3-year software and 4-year hardware technical refresh cycle, and may be updated through ‘product replacement’ prior to the release of a new increment. Through spiral development, successive increments will, such as CENTRIXS-M BLK II Increment II (BLK II/II), will incorporate new equipment, interfaces, and additional CDS capabilities, which will expand on the capabilities of the CENTRIXS nodes (SPAWAR, 17, 2007). Refer to Figure 20 and Table 5 for a graphic depiction of the above discussion.

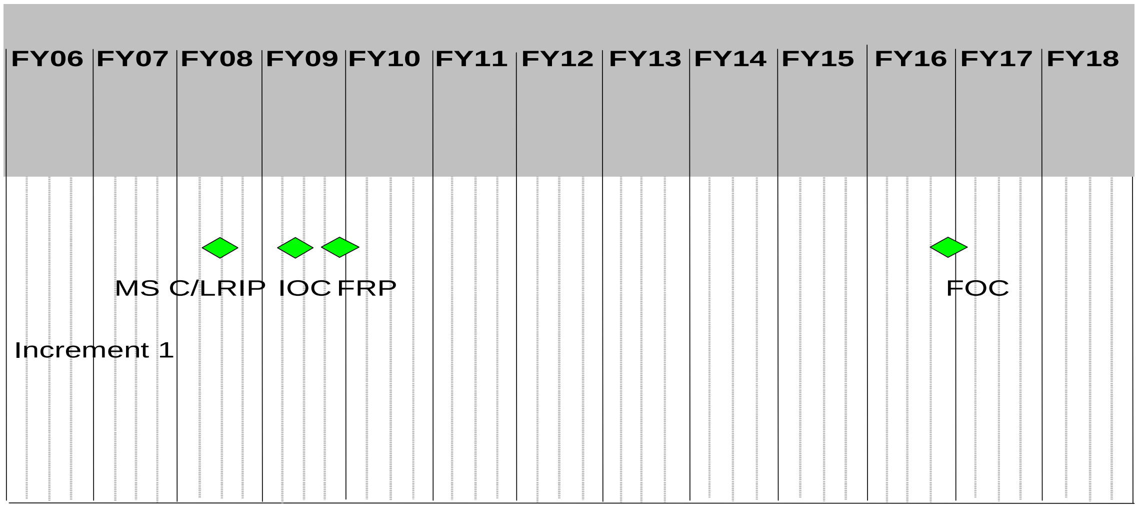


Figure 20. CENTRIXS-M BLK II/I development schedule (From: Soriano, 2007)

Table 5. CENTRIXS BLK II/I and BLK II/II development schedule

Schedule FY Profile	FY 2006	FY 2007	FY 2008	FY2009
Milestone C – Block II/I			2Q	
Initial Operational Capability			4Q	
Full Rate Production				2Q
System Development – Block II/II	1Q-4Q	1Q-4Q	1Q-4Q	1Q
Operational Assessment		4Q		
Development/Operational Tests				1Q

CENTRIXS is an interim legacy system being fielded to meet a serious need until a Joint replacement such as a MNIS or a Coalition Information Sharing (CIS) system can be developed and fielded. CENTRIXS is related to CENTRIXS Global in that they share applications, are IP-based systems and use the GIG for communications. CENTRIXS Global and CENTRIXS do not have approved ICDs. The approved CENTRIXS Global Information Support Plan (ISP) does not identify CENTRIXS Global as either a Family of Systems (FoS) or Systems of Systems (SoS). The CENTRIXS system meets the definitions of an IT system. The CENTRIXS program will only include the acquisition of the hardware and software required to perform the capabilities identified in this CPD. The CENTRIXS system will be required to interface with, but not acquire existing and new domains and networks (SPAWAR CPD, 9, 2006.)

CENTRIXS is a mission essential information system and Quality of Service (QoS) requirements will be further identified and defined by the ISP. Significant CENTRIXS capabilities have been fielded to date with the Block 0, 1 and 2 builds. The Increment 1 build is intended to consolidate and coordinate the execution of U.S. and Multinational CENTRIXS system capabilities. The Increment I capability will be achieved by upgrades to specific systems, replacement of legacy systems, and introduction of new systems. The NSS and IT supportability requirements will be identified in both the program ISP and Acquisition Strategy (AS.) The CENTRIXS system program will provide the NSS and ITS support for all Increment I systems.

CENTRIXS is quickly becoming the center piece for coalition communications. Therefore, the timely acquisition, installation, accreditation as well as Life Cycle Support (LCS) of CENTRIXS are crucial to the success of the program. The PM, PMW-160, is working hard to achieve full POR status for CENTRIXS. Hardware for procurement and development of ISNS is under the cognizance of PEO C4I/Space PMW-160 as well as OPNAV (N71). The Assistant PM for CENTRIXS is the Program Executive Officer, C4I in San Diego, California. The Assistant Program Manager is responsible for the development, fielding, and life cycle support of the Navy's CENTRIXS system (JCS, 2, 2006.)

Version 2.0 of the CPD, the first JCIDs document produced for CENTRIXS BLK II/I adds increased capability to an already mature system and will enter the acquisition process post Milestone B. Since the BLK II/I revision will occur after Milestone B, there is no associated ICD, CDD, or Design Readiness Review (DRR) associated with the revised CPD. CENTRIXS BLK II/I capabilities were derived from requirements outlined two primary documents, the joint GIG Mission Area ICD and the MNIS ICD. The CENTRIXS program is approaching a Milestone C decision by the MDA and the PM is preparing the CPD prior to JROC review (Soriano, 24, 2007.)

CENTRIXS Block 2, Increment I installation consists of two afloat variants, one for unit level platforms and one for force level platforms. The unit level platforms have more restrictive SWaP requirements and therefore require a smaller CENTRIXS system footprint. In order to reduce SWaP, the CENTRIXS hardware suite aboard unit level platforms consists of a single rack version of the hardware suite aboard force level platforms. The reduction in hardware amounts to a reduction in the number of enclaves that a user can access simultaneously. Unit level platforms will only be able to access 4 enclaves vice the 5 enclaves for force level platforms.

CENTRIXS Increment 1 also contains a shore variant, which will reside at the PRNOC and the UARNOC. The shore variant, a component of CENTRIXS, provides the afloat platforms with the ability to exchange information and monitor network performance and connectivity with allied and coalition partners, by providing access to Coalition Networks, as well as CENTRIXS Global via (mail guards, cross-domain chat server, and air-gapping workstations). The CENTRIXS BLK II/I, shore variant is similar to the afloat system but contains additional equipment such as concentrators and has more servers. Both shore facilities, PRNOC and UARNOC, maintain a fully redundant back-up capability. Eventually, afloat units will be able to connect into any of the Regional NOCs and receive the same services being provided by the initial two shore facilities. The shore NOCs also act as the main interface to the DISA Global CENTRIXS Wide Area Network. The shore NOCs also have the capability to build various CENTRIXS COIs on an as required basis in order to support real world events and exercises.

An estimated 113 systems (111 afloat and 2 ashore) will be required to satisfy operation requirements for afloat platform installations. These numbers will change as warfare sponsors change deployment, commissioning, and decommissioning schedules. The ship quantities are current goals only and are subject to change. Changes in the quantity of ships will not require a change in this CPD. In addition, objective drop quantities will change as the systems and fleet requirements evolve. CENTRIXS Increment 1 will be provided to the following ship classes and shore sites as depicted in Table 6 (Soriano, 12, 2007).

Table 6. CENTRIXS-M BLK II/I Installation Plan by Platform

Platform	CENTRIXS-M Variant	Number of Clients	Quantities
Aircraft Carrier - Nuclear (CVN)	Force Level	30	8
Amphibious Assault (LHA)	Force Level	30	2
Amphibious Assault (LHD)	Force Level	30	6
Amphibious Command (LCC)	Force Level	30	2
Amphibious (LPD)	Unit Level	15	8
Guided Missile Cruiser (CG)	Unit Level	15	22
Guided Missile Destroyer (DDG)	Unit Level	15	63
Network Operation Center (NOC)	Shore Variant	Variable	2

CENTRIXS shall be developed and acquired (in accordance with DoDI 5000.2) in increments providing increased functionality of CDS capabilities with succeeding increments. The threshold target date for IOC attainment is the fourth quarter FY2009. The objective target date for IOC attainment is the second quarter FY2009. IOC for each CENTRIXS increment is defined as the first attainment of a CENTRIXS system of approved specific characteristics that is operated by adequately trained Naval and civilian personnel. FOC is attained for each increment when all units designated to receive the increment are fully equipped with the authorized system, as defined above, for IOC.

Currently, the Pacific Region Network Operations Center (PRNOC) is the only network hub for all CENTRIXS connectivity. CENTCOM has directed that all ships deploying to NAVCENT AOR have CENTRIXS capability. At present, 153 Navy deployable warships have coalition connectivity. This includes a separate shipboard coalition LAN/WAN with respective infrastructure, servers and work stations. Under current procurement and installation funding, FOC for CENTRIXS is 2018. These organizations work together to identify and implement the latest technologies, CENTRIXS BLK II/I in order to ensure proper implementation into the program. Engineering, development, integration, installation, training and life cycle support will be accomplished through Navy and Defense Department activities (Soriano, 2007.)

CENTRIXS BLK II/I became a PMW-160 POR in first quarter of FY06 and is planned for Milestone C review and LRIP in FY2008. The current CENTRIXS configuration uses Trusted Solaris 8.x for combining multiple coalition enclaves and distributing data to Multi-Level Thin Client devices resulting in decreased hardware/footprint by no longer requiring separate clients and back end servers for each enclave. The CENTRIXS BLK II/II architecture is still under development and testing, and once operational, will provide a single hardware platform with virtualized domains to contain variable numbers of coalition COIs, which also provide separation of data in transit and at rest using Virtual Machine processing and encrypted hard disks.

The Joint Interoperability Test Command (JITC) is in the process of conducting a global Interoperability Certification on CENTRIXS. The JITC will directly observe or simulate testing and utilize any available test data from Developmental and/or

Operational Tests conducted by any of the COCOMs or the Program Office. Upon completion of testing, JITC will conduct a thorough analysis of all the test data gathered during the CENTRIXS Interoperability Test Phase. An Interoperability Certification Evaluation Test Report will be provided to the DISA MNIS Joint Program Office (JPO) upon completion of the analysis. An Interoperability Certification Letter will be drafted based on the outcome of the Interoperability test data and will be forwarded to the JITC Certification Panel for their review and approval (MIP, 2007.)

The JITC maintains a CENTRIXS test network, which includes a command headquarters configuration and various deployable configurations. We also maintain various NSA-approved type I encryptions devices, including the KG-175 TACLANE and KIV-7, and a data link simulator, which facilitates simulation testing of the live CENTRIXS network in a lab environment. This test network is also used to test Information Assurance Vulnerability Alerts (IAVA) for the DISA MNIS JPO, prior to enterprise-wide deployment (JTCI, 2007.)

D. INSTALLATION

There are four operational CENTRIXS variants: Block 0, Block I, Block II and Block II/Increment I (BLK II/I) and Block II/Increment II (BLK II/II). The BLK II/II is still under development and will therefore be mentioned only briefly. As of May 2007 there are 153 ships fielded with CENTRIXS capability, 129 Block 0, 20 Block I and 4 Block II. Over 130 installations were completed in FY2006, expanding the CENTRIXS-M footprint from zero to nearly three fourths of all Navy platforms in a single calendar year. The CENTRIXS program provides a network infrastructure that allows simultaneous access to multiple coalition WANs and incorporates the Common PC Operating System Environment (COMPOSE), which provides a server and client operating system environment for other applications and collaborative tools such as Same time Chat, Domino, and C2PC as means to share a COP and exchange information using Collaboration At Sea (CAS). The CENTRIXS program uses both COTS hardware and software and Open Standards to maximize commercial technology and support. In-service engineering and technical support ensures existing systems are upgraded and modified to keep pace with current technology and industry (PMW-160, 2, 2006.)

In addition to the 153 platform installations scheduled for FY2006, there are also two different portable systems available. The two portable variants are the CENTRIXS Fly-Away Kit (CFAK) or (FAK), which comes with a portable INMARSAT unit providing 24/7 connection at 64K and the CENTRIXS Portable Operation Kit (CPOK), which connects via an Iridium telephone at 2.4 Kilobits and are shown below in Figures 21-23. The CPOK is much more mobile but not as robust as the CFAK. The CFAK or FAK is being deployed to Fleet Commanders on an as needed basis to support coalition communications requirements. The CENTRIXS Inter-Service Engineering Activity (ISEA) has developed a Life Cycle Management plan to strategically oversea and support the FAK. The FAK is being fielded to NECC (PMW-790) and follow on deliveries are scheduled for MOC, JMAST and Tactical Mobile (PMW-180) and the ISEA will providing training and sustainment for units being fielded.

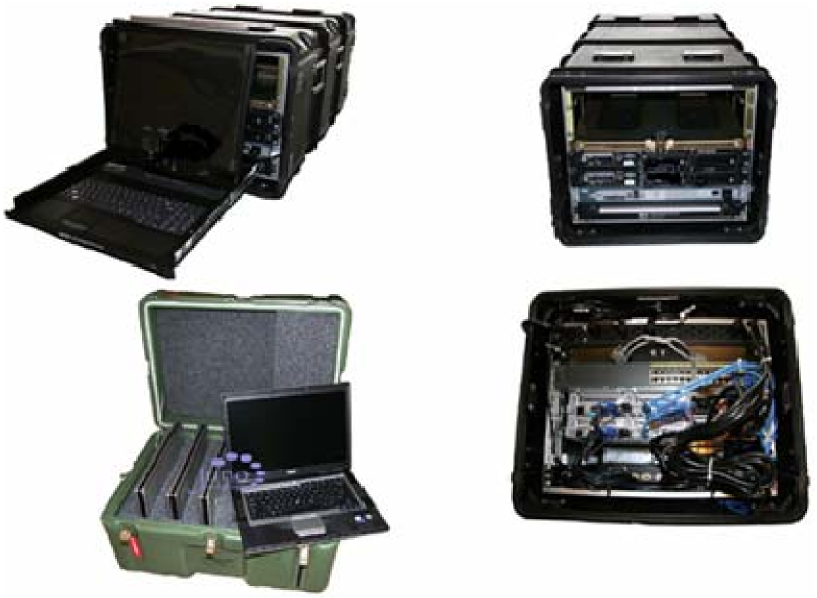


Figure 21. CENTRIXS Fly Away Kit (CFAK) (From: Soriano, 24, 2007)

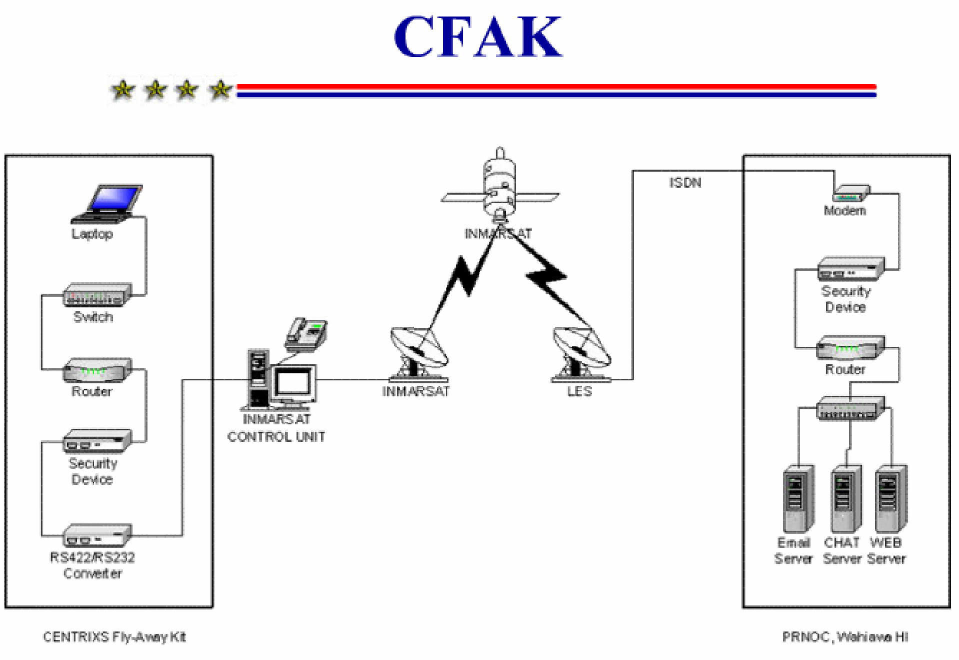


Figure 22. CFAK Architecture (From: SPAWAR Master Series, 2007)

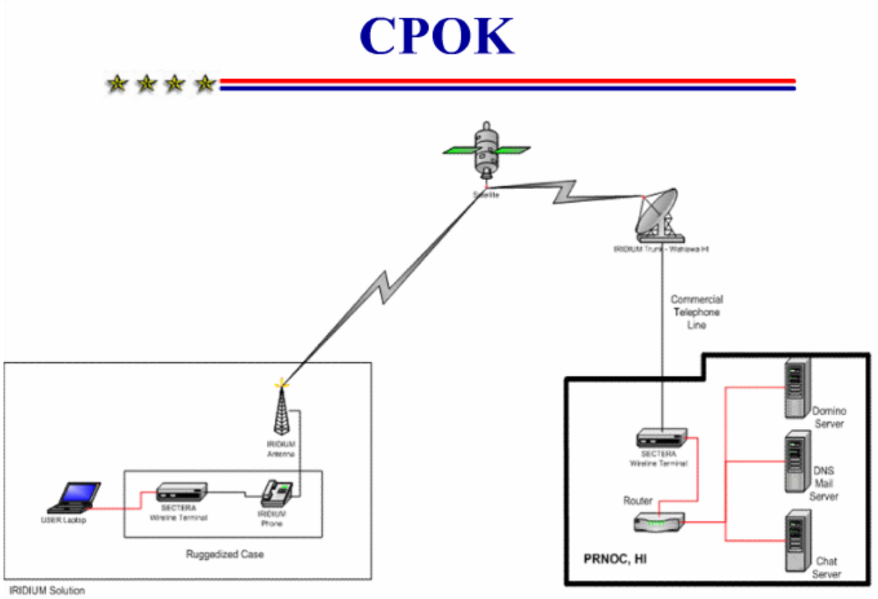


Figure 23. CPOK Architecture (From: SPAWAR Master Series, 2007)

The Standard CENTRIXS enclave build (Tables 7 and 8) represent the typical server, workstation and software installation.

Table 7. CENTRIXS Standard Enclave Server Build (From: Shannon, 2007)

Servers	Domain Controller - Windows 2000/2003 Server; Active Directory; DNS; SAV Corporate Edition; MS Office 2003.
	Exchange - Windows 2000/2003 Server; Exchange 2000; MS Office 2003.
	DNSMAIL- RedHat Linux 9.0; Sendmail.
	NT/MGT - Windows 2000/2003 Server; SAV Corporate Edition; Cisco TACACS; SolarWinds TFTP Server; SecureCRT 4.1; MS Office 2003; Whatsup Gold Server 9.0; SameTime Chat; NTP Server.
	Domino - Windows 2000; Lotus Domino; and SameTime Chat Server.
	Call Manager - Windows 2003; Cisco CallManager 4.1; MS SQL Server.
	SUS - Windows 2000/2003; MS Systems Update; MS SQL Server; SAV Corporate Edition Server w/System Center Console and SecureCRT 4.1.

Table 8. CENTRIXS standard enclave workstation build (From: Shannon, 2007)

Workstations	WUG - Windows 2000/XP Pro; SAV Corporate Edition; SecureCRT 4.1; MS Office 2003.
	Workstation - Windows 2000/XP Pro; SAV Corporate Edition; SecureCRT 4.1; MS Office 2003; SameTime Chat.

1. Block 0

The typical Block 0 or unit level installation nomenclature is AN/USQ-185(V1) and the installation consists of a three servers with removable hard drives, Primary Domain Controller (PDC) or (DC1), Backup Domain Controller (BDC) and a Dell D610 Laptop Domino/Collaboration At Sea (CAS) Server. Domain Controller One (DC1) is the PDC and configured with DNS, IIS Server, and the Sametime Chat Client. Domain Controller Two (DC2) or the BDC is configured with DNS, MS Exchange and the Sametime Chat Client. The configuration also includes a CISCO 2611XM Router, five port Hub, Alcatel 4024 Switch, KG-175 TACLANE, three DELL GX520 Workstations and a UPS. Some Block 0 and Block I installation can include up to 10 workstations. The KG-175 TACLANE is then interfaced to the ADNS using a Cisco 3745 Router or

Proteon CNX-500 Router. The ADNS is the further encrypted using a KG-194 TRANSEC before the information leaves the ship. The software load for the PDC, BDC, Lotus Domino Client and Workstation is GOTS-D4.1.1.2. The CENTRIXS Block 0 installation is designed for small unit level platforms, which have been designated as: AOE, ARS, AS, DD, DDG, CG, LPD, LSD, MCM, MHC and FFG (Soriano, 2007.)

The nomenclature for the Preventive Maintenance System is AN/USQ-153B(V)6 Block 0, which is different from the system nomenclature. The PDC and BDC are typically installed in Radio Central and a laptop is loaded with the Lotus Domino Client, Collaboration At Sea (CAS), and maintained in Radio under lock and key. The laptop is primarily for replication but is often loaded with the workstation software and used as another or backup workstation. The PDC and BDC are also normally loaded with the workstation software so they can be used as both a server and a workstation. Therefore, the Block 0 installation consists of three severs and three workstations providing access on three workstations to a single CENTRIXS enclave (MIP, 2007.)

Table 9 outlines the prerequisite training and knowledge required by ships force personnel to maintain the system. It is important to acknowledge the specific rate training the personnel have received as part of their core Class “A” and “C” school training as well as the training they receive as part of the CENTRIXS installation training. The In-Service Engineering Activity (ISEA) will ensure training proficiency through Computer Based Training and Courseware, with Courseware being the long term solution. The ISEA has acknowledged there is a training gap and that the unit level training needs to be addressed earlier in the schedule. In addition, the ISEA has acknowledged a KM training shortfall, which needs to be, addressed (Soriano, AFCEA, 2007.)

Table 9. Prerequisite training and SPAWAR CENTRIXS-M installation training for ships force personnel (From: Shannon, 2007)

PLATFORM Average Clients Average Number of Personnel	Operators (3, 10, 30) (3)	Maintainers (1-2) (2)	System Admin (1-2) (1)	Web Admin (0-1) (1)	Training Days x Personnel x Terminals
SURFACE 111 BLK II/I Clients	Install OJT - 1 wk JQR/PQS - 4 hr	ISM NEC - 12 wks Install OJT - 1 wk JQR/PQS - 4 hr	JNC PREREQ – 6 wks P/O ISNS SM - 2 wks Install OJT - 1 wk Module - 3 days	Install OJT - 1 wk Class/lab - 3 days	
SHORE 2 Clients			JNC PREREQ - 6 wks Install OJT - 1 wk MTT REFTRA - 1 wk	Install OJT or MTT REFTRA - 1 wk Class/lab - 3 days	
CENTRIXS Training Days per person	6 Days	66 Days	48 Days	8 Days	128 Days
Prerequisite A & C School	0 Days	730 Days	365 Days	180 Days	1275 Days
Training Per Person	6 Days	796 Days	413 Days	188 days	1403 Days
Total Training Days x number of personnel per Node	6 Days X 3 18 Days	796 Days X 2 1592 Days	413 Days X 1 413 Days	188 Days X 1 188 Days	Total days training per node 2206 Days

The ship does not gain any additional personnel or billets for operating or maintaining the system as part of the installation. The ship normally assigns Operation Specialists (OS) and Information System Technicians (IT) the responsibility of operating the system while Electronic Technicians (ET) normally maintaining the system. Since the ship assigns operators and maintainers the enlisted ratings as well as pay grades assigned varies from ship to ship. System Administrators responsibilities are typically assigned to ships force personnel who are already performing system administration duties and responsibilities for the ship. However, web administrators are normally not required or assigned for unit level installations. If the platform has embarked staff then the ships Web administrator is trained on configuring the CAS site. SPAWAR is preparing a Naval Training Support Plan (NTSP), which has proven challenging since there are defined roles with different training paths. The two training paths are the Fleet Installation Training (FIT) and Shore Installation Training (SIT) (Shannon, 2007.)

SPAWAR has leveraged heavily off the existing ISNS training enlisted personnel receive and focuses on difference training. SPAWAR is in the process of restructuring the prerequisite knowledge exams for enrollment in the training since overlooking the prerequisite requirements in the past has lowered the level of training for entire class. The system uses the standard COMPOSE software load which further enables SPAWAR to use difference training. The average total cost for a CENTRIXS Block 0 installation is $1.5M, $500K for materials, $500K for installation and $500K for accreditation. In addition, SPAWAR budgets $7,500 per installation for training ships force personnel on system operation and maintenance (MIP, 2007.)

2. Block 1

The typical Block 1 or force level installation nomenclature is AN/USQ-185A (V1) and the installation consists the installation consists of a three servers with removable hard drives, PDC or (DC1), BDC and a Dell D610 Laptop Domino/Collaboration At Sea Server. Domain Controller One (DC1) is the PDC and configured with DNS, IIS Server, and the Same-time Chat Client. Domain Controller Two (DC2) or the BDC is configured with DNS, MS Exchange, and the Same-time Chat

Client. The configuration also includes a CISCO 2611XM Router, five port Hub, Alcatel 4024 Switch, KG-175 TACLANE, three DELL GX520 Workstations and a UPS. Some Block 0 and Block I installation can include up to 10 workstations. The KG-175 TACLANE is then interfaced to the ADNS using a Cisco 3745 Router or Proteon CNX-500 Router. The ADNS is the further encrypted using a KG-194 TRANSEC. The software load for the PDC, BDC, Lotus Domino Client and Workstation is GOTS-D4.1.1.2. The CENTRIXS Block 1 installation is designed for force level platforms, which have been designated as: CV/CVN, LHA, LHD, AGF and LCC (Soriano, 2007.)

The nomenclature for the Preventive Maintenance System is AN/USQ-153B(V)6 Block 1 which is different from the system nomenclature. The PDC and BDC are typically installed in Radio Central and a laptop is loaded with the Lotus Domino Client, CAS, and maintained in Radio under lock and key. The laptop is primarily for replication but is often loaded with the workstation software and used as another or backup workstation. The PDC and BDC are also normally loaded with the workstation software so they can be used as both a server and a workstation. Therefore, the Block 1 installation consists of three severs and ten workstations, each server and workstation has three removable hard drives.

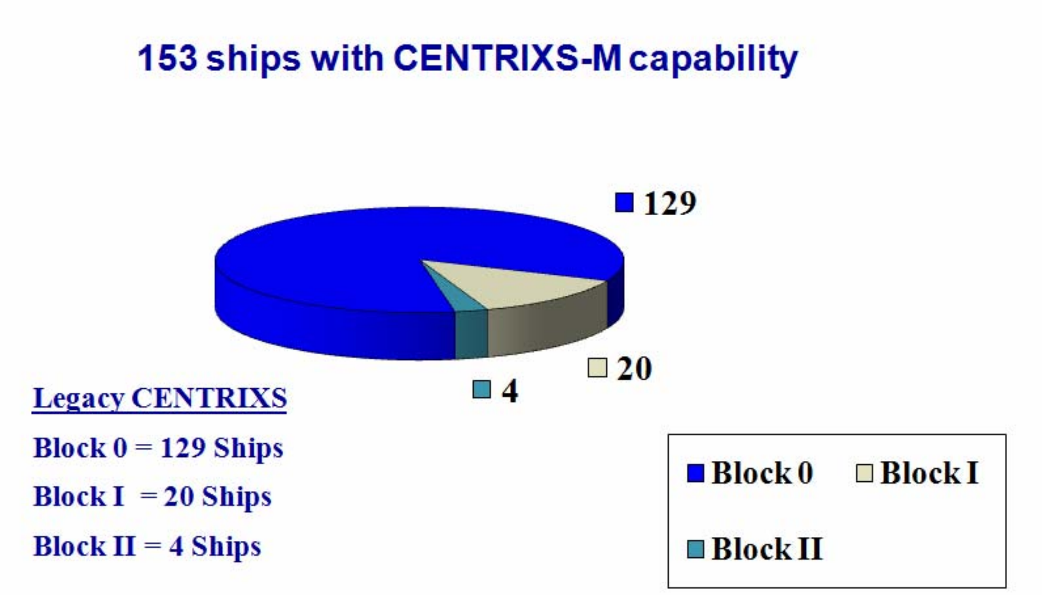


Figure 24. CENTRIXS Installations as of 23 May 2007 (From: Soriano, 8, 2007)

A CENTRIXS Block I system was installed upon the USS ABRAHAM LINCOLN (CVN) and the system included three workstations in Radio Central but the ship purchased an additional 15 workstations which were also configured with the workstation client software. The COMPOSE software load was used to configure the DNS, EX, and WINS servers. As with the CENTRIXS Block 0 installation the workstation software which contains Microsoft Office was loaded onto the servers so they could also function as workstations. The average installation, accreditation and training cost for Block 1 installation is virtually identical to the average cost of a Block 0 installation, a total cost of $1.5M (Shannon, 2007.)

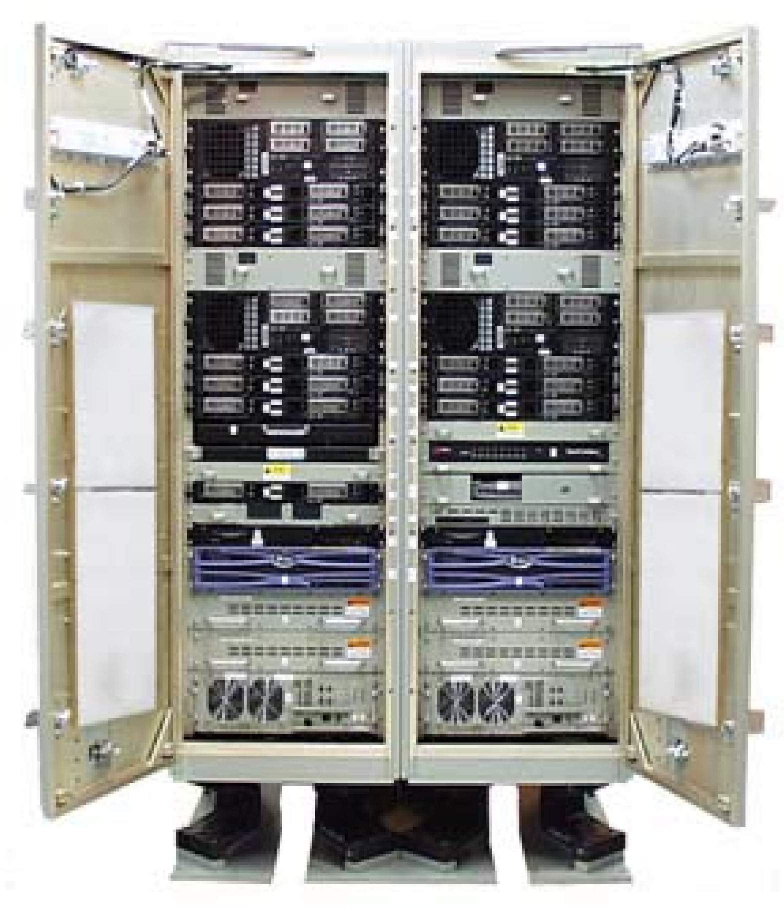
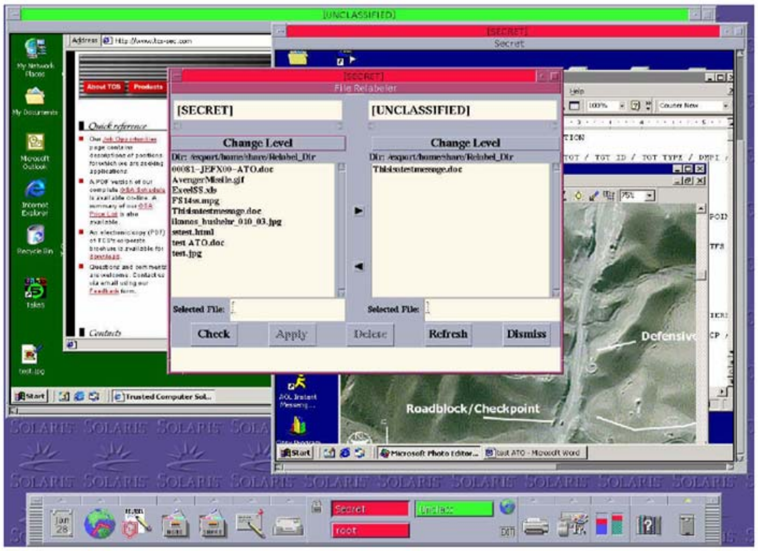


Figure 25. CENTRIXS-M Block II Multi-Level Thin Client (MLTC) Dual Rack (From: Soriano, 10, 2007)

3. Block II

The Block II installation is the new command ship installation and the nomenclature is the AN/USQ-185(V2). The Block II installation incorporates the Multi-level Thin Client (MLTC) architecture, which reduces SWaP. The MLTC virtual workstation supports simultaneous access to four coalition enclaves and SIPRNET. The Block II installation is designed for LCC and CV/CVN platforms and is comprised of a PDC, BDC and a Laptop Domino Server. The configuration also includes a CISCO router, Omni-stack switch, KG-175 TACLANE, 30 Ultra-Thin client terminals and an UPS. The software load for the PDC, BDC, Lotus Domino Client and Workstation is GOTS-D4.1.1.2. The COMPOSE load was used to configure the DNS, EX, and WINS servers. The Block II version is scheduled to be accredited in FY09 using the Sun Solaris 10 TX/CONET 2.0 software. A total of 24 Force Level (FL) installations are scheduled and five installations will be completed in FY07. The average installation, accreditation and training cost for Block I installation is virtually identical to the average cost of a Block 0 and a Block I installation which is $1.5M (Shannon, 2007.)



Enclave classification is displayed in window header

Enclave access is based on Smart Card authorization

User only required to login one time

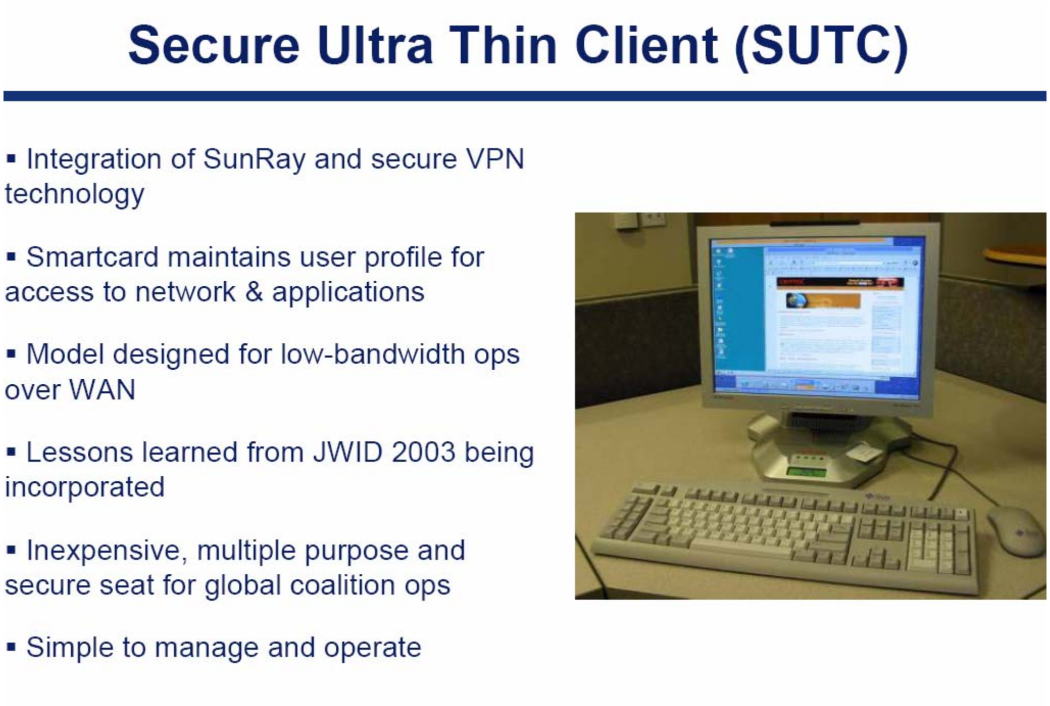
System does not allow data transfer between security enclaves

Unclassified – For Demonstration purposes only

Figure 26. CENTRIXS Block II (MLTC) Demonstration (From: Soriano, 11, 2007)

4. Block II Increment I

The Block II Increment I, BLK II/I, installation provides a network infrastructure, which enables simultaneous access to multiple Coalition WAN and incorporates the COMPOSE. COMPOSE provides a server and client operating system environment for other applications and collaborative tools such as Same-time Chat, Domino and C2PC as means to share a COP and exchange information using CAS. The CENTRIXS program uses both COTS hardware and software and Open Standards to maximize commercial technology and support. In-service engineering and technical support ensures existing systems are upgraded and modified to keep pace with current technology and industry. The BLK II/I installation increases the number of Unit Level (UL) clients from 10 to 15 UTC and uses a single rack configuration.



Secure Ultra Thin Client (SUTC)

- Integration of SunRay and secure VPN technology
- Smartcard maintains user profile for access to network & applications
- Model designed for low-bandwidth ops over WAN
- Lessons learned from JWID 2003 being incorporated
- Inexpensive, multiple purpose and secure seat for global coalition ops
- Simple to manage and operate

Figure 27. Ultra Thin Client (UTC) consists of a Monitor, Keyboard and Mouse (From: SPAWAR, 2003)

The FL version increases the number of clients from 10 to 30 and uses a dual rack configuration similar to the Block II design.. Accreditation of the BLK II/I will require new hardware components and a new operating system (Sun V245 and Solaris 10 TX).

The installation schedule has 27 systems being fielded in FY09, 37 in FY10 and 36 in FY11. This upgrade is in support of GWOT operations. Joint Worldwide Intelligence Communications System (JWICS) capability will be installed on CENTCOM AOR deployed submarines (Department of the Navy Publication, 2007).

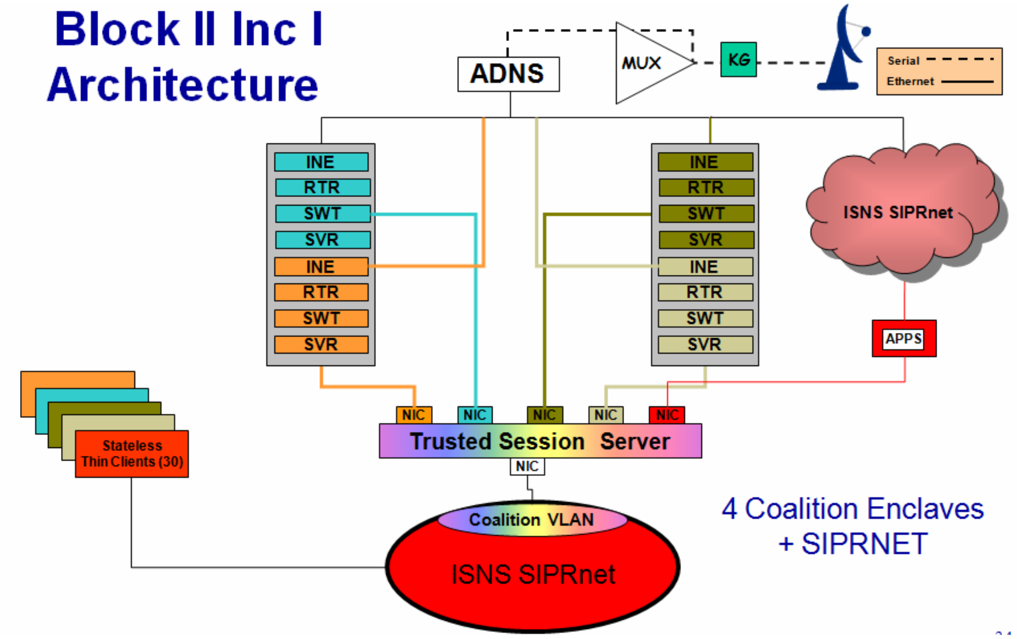


Figure 28. CENTRIXS Block II/Increment I, FL Architecture (From: Soriano, 34, 2007)

5. Block II Increment II

The future CENTRIXS BLK II/I installation will eventually provide a single hardware platform with virtualized domains to contain variable numbers of coalition COIs, which also provide separation of data in transit and separation of data at rest using Virtual Machines (processing) and encrypted hard disks. The future CENTRIXS BLK II/II installations will produce solutions, which will leverage the Consolidated Afloat Network and Enterprise Services (CANES) capability. Eventually CANES will be the single network provider and integrate all UNCLAS, Coalition to SCI. CANES will reduce cost by eliminating existing standalone/legacy networks and will provide an adaptable solution for meeting our rapidly changing warfighting requirements. Further, CANES will reduce shipboard footprint, SWaP, and overall lifecycle management costs.

The support for CANES is based on the requirement to reduce the number of networks, providing efficiency through a single engineering focus on technical solutions. CANES will streamline the acquisition, contracting, and testing events, and eliminate the inefficiencies associated with managing multiple Configuration Management (CM) baselines, logistics and training "tails" into a unified support structure. See Figure 29 below for a graphic of the road ahead. CANES will be developed and deployed using a highly innovative and competitive business strategy guaranteeing best value to the government and best solution for the Sailor (Department of the Navy Publication, PEO C4I, 2006.)

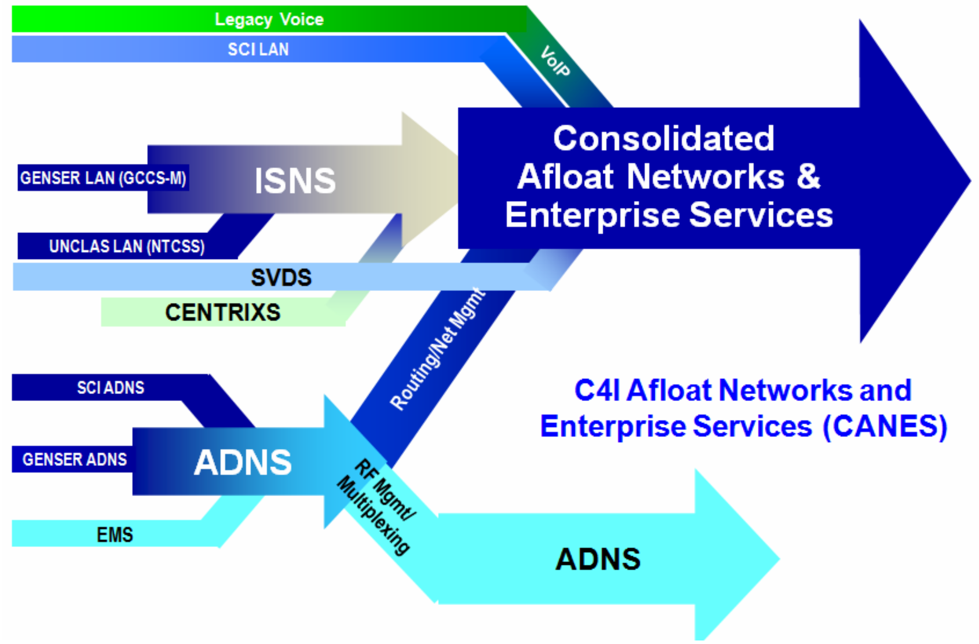


Figure 29. CANES Roadmap (From: Dept. of the Navy PEO C4I, 2006)

6. Network Operation Center (NOC)

The two shore Network Operation Centers are the PRNOC and the Unified Atlantic Region Network Operations Center (UARNOC). The CENTRIXS installation at UARNOC was completed third quarter FY07. PRNOC and UARNOC support the fleet by providing network monitoring and troubleshooting, help desk, DNS services, Mail services, Mail guard administration support. The PRNOC CENTRIXS operations support consists of one NNWC Engineer, three CENTRIXS In-Service Engineering Activity (ISEA) Engineers, one Operations Manager, three Operations Group Leads, nine Network Operators (two to three watch standers per shift) and four CAS Web administrators (one watch stander per shift). The CENTRIXS operations support hours are 0600-2300 seven days a week. The PRNOC CENTRIXS applications consist of SMTP/POP Email, DII Mail Guard, VOIP, C2PC and CAS, which also includes Persistent Chat, Same-time Connect/Web Chat, Domino Web and Domino Email (Soriano, 2007.)

The primary hidden cost drivers which impact the overall installation costs are the type and condition of the platform, location where the installation is being performed and the amount of reuse included in the installation. The average cost of an operational Block 0, Block I and Block II platform including the equipment, installation and accreditation is $1.5M. There was insufficient unclassified data available to break down the cost by Unit Level and Force Level installations. Further, there was insufficient information available to provide an estimate for the BLK II/I and BLK II/II installation costs (Soriano, 2007.) See Appendix H for typical PRNOC connectivity diagrams.

E. ACCREDITATION

System Accreditation is a challenge and is difficult to execute a under extended accreditation cycles. Certification test and evaluation takes an average of 18 Months for medium priority systems. Therefore, a reduction in the accreditation timeline is critical to fielding the system on schedule. One potential solution is to use an as-is or incremental approach, modifying components which have already been accredited. Another challenge will be attaining Common Criteria Certification for security critical components prior to use in DoD acquisition or development. Secret and Below Interoperability (SABI) Certification is another drawn out process, however, prior SABI Certifications on systems being upgraded will reduce the time required for accreditation.

Systems, which have already been fielded and are operational, will require accelerated re-accreditation. Accelerated re-accreditation will be required for changing enclaves, adding new enclaves, modifying or adding to fielded applications and changes in security policy. The existing security tool such as DITSCAP, which is now known as the DoD Information Assurance Certification and Accreditation Process (DIACAP) and SABI-CDS provide the guidance required for commands to achieve full accreditation. The DIACAP instruction was placed into effect July 06, 2006 and a 180 day period was outlined to transition from DITSCAP to DIACAP (DIACAP, 2006.)

SABI is an Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C31) mandated, Joint Chiefs of Staff, Command, Control, Communications and Computer Systems (JS/J6) sponsored Information Assurance initiative, which improves the security posture of all secret and below DoD systems because it utilizes a community-based risk acceptance approach, uses proven information systems engineering principles and encourages the reuse of proven information security solutions. The goal of SABI is to ensure secure secret and below interoperability solutions for the war fighter within community-acceptable risks. CENTRIXS will have an open SABI ticket during the SABI certification process.

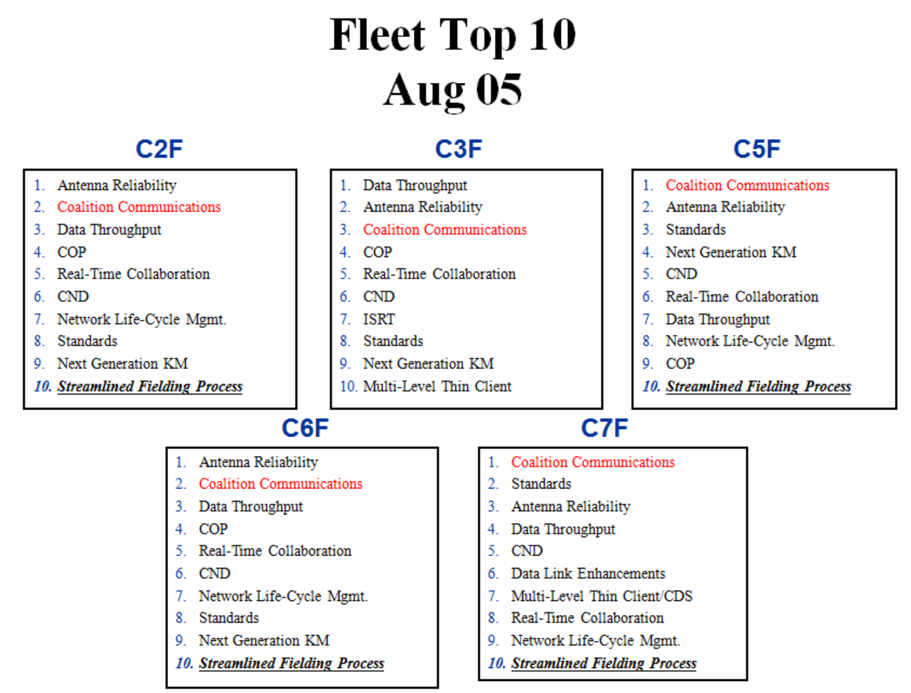
Another version of SABI is Top Secret and Below Initiative (TSABI) is a critical component of the latest CENTRIX Block II accreditation process and is founded on Information System Security Engineering (ISSE) principles whereby information systems security (INFOSEC) is integrated as a part of systems engineering and systems acquisition processes, strong customer participation in support of mission needs, and the optimal use of INFOSEC disciplines to provide security solutions. Documentation implements the DoD Instruction 5200.40, DITSCAP. The SABI process teams the local site customer with appropriate engineering, risk, vulnerability, training and programmatic community risk-focused support necessary to develop the right solution for the customer's SABI requirement. SABI maintains this community team throughout the system security engineering process. This strengthens the community risk acceptability of a specific site solution through continued dialog and participation of all relevant stakeholders (SABI, 1998.)

The Director of Central Intelligence Directive 6/3 and the System Security Authorization Agreement (SSAA) are vital to achieving system accreditation. The SSAA is a formal agreement between the Designated Approving Authority (DAA), the Certification Authority (CA), and User Representatives resulting in certification and accreditation approval. The SSAA is to be used throughout the lifecycle of the system to guide actions, document decisions, specify security requirements, and maintain operational security. The SSAA is a living document that undergoes reviews to record any changes made which may affect the accreditation status of the system. The SSAA verifies the system mission, environment, and architecture. It identifies threats to the system and documents compliance with Certification and Accreditation (C&A) security requirements. The SSAA evaluates the lifecycle and documents all constraints and vulnerabilities of the system. The SSAA ensures the CA and DAA are aware of vulnerabilities within the system and allow for operation with an acceptable level of risk, culminating in the accreditation of the system. Each installation must have a unique SSAA as part of the accreditation package (SABI, 1998.)

The CENTRIXS program must remained aligned with existing DoD activities such as Unified Cross Domain Management Office (UCSMO) which maintains an inventory of all CDS, Navy Cyber Defense Operations Command (NCDOC), Joint Task Force-Global Network Operations (JTF-GNO) and MNIS, which all fall under the umbrella of DoD coalition networks. Accreditation is the most difficult and time consuming component of a CENTRIXS installation.

F. CHALLENGES

The budget for the next three years appears to introduce a considerable challenge to the program with a drastic reduction in funding, over one sigma, in FY2008 and FY2009. The FY2007 O&M budget of $268 million is followed by the planned budgets of $25.34M in FY2008 and $24.7M in FY2009. Not to mention the recent $5.8M augmentation in FY2007 to increase the number of clients per installation. With 153 existing installations and only four CENTRIXS Block II installations completed as of the first quarter FY2007 it is unlikely the program will be able to field the scheduled installations from FY2008 through FY2011. The fielding schedule for the BLK II/I calls for 27 installations in FY2010, 37 for FY2010 and 36 for FY2011. The aggressive fielding plan does not correspond to the drastic reduction in program funding. See Figure 29 for a graphic of Fleet Commanders Top 10 C4I priorities (FCW, 2007.)



Fleet Top 10
Aug 05

C2F

1. Antenna Reliability
2. Coalition Communications
3. Data Throughput
4. COP
5. Real-Time Collaboration
6. CND
7. Network Life-Cycle Mgmt.
8. Standards
9. Next Generation KM
10. ***Streamlined Fielding Process***

C3F

1. Data Throughput
2. Antenna Reliability
3. Coalition Communications
4. COP
5. Real-Time Collaboration
6. CND
7. ISRT
8. Standards
9. Next Generation KM
10. Multi-Level Thin Client

C5F

1. Coalition Communications
2. Antenna Reliability
3. Standards
4. Next Generation KM
5. CND
6. Real-Time Collaboration
7. Data Throughput
8. Network Life-Cycle Mgmt.
9. COP
10. ***Streamlined Fielding Process***

C6F

1. Antenna Reliability
2. Coalition Communications
3. Data Throughput
4. COP
5. Real-Time Collaboration
6. CND
7. Network Life-Cycle Mgmt.
8. Standards
9. Next Generation KM
10. ***Streamlined Fielding Process***

C7F

1. Coalition Communications
2. Standards
3. Antenna Reliability
4. Data Throughput
5. CND
6. Data Link Enhancements
7. Multi-Level Thin Client/CDS
8. Real-Time Collaboration
9. Network Life-Cycle Mgmt.
10. ***Streamlined Fielding Process***

Figure 30. Trident Warrior 2005, Fleet Commanders Top 10 C4I Priorities (From: Trident Warrior Lessons Learned, 2005)

As the DoD continues to moves to toward more joint and coalition operations CENTRIXS is becoming even more critical since it provides the capability to operate with coalition forces at various levels of classification. With the coalition demand increasing the CFAK is becoming popular choice for commanders to gain interoperability for short term exercises or operations. However, the CFAK was designed as a emergency surge gap filler and the program is not designed to support long term commitments. Therefore, as more units are fielded on U.S. platforms there will be a reduction in the number of CFAK requests. In turn we need our coalition partners to also commit to investing in installing the CENTRIXS systems on their ships to prevent a over dependence on the CFAK option.

The FY2008 budget request shifts responsibility for CENTRIXS from the Navy to DISA. Changes in program responsibility typically cause an adverse impact the program schedule by creating a lag as the new personnel get up to speed. However, this should not be the case with DISA since they have been involved with CENTRIXS and are familiar with the program and issues (Brewin, 1, 2006.)

Maintaining the gap between program development and advances in technology appears to be the critical challenge for CENTRIXS. Since IT systems take an average of 10 years to field and with technology doubling every 18 months we continually field systems which miss the mark and are up to six generations behind the technology we need today. CENTRIXS is not an exception to the trend of lagging fielding lagging technology but DoD is doing better than many other sectors at keeping up with the technology curve.

G. CONCLUSION

The CJCS identified our coalition communications during Trident Warrior 2006 as, “Inadequate Ability to Share Operational Information with Mission Partners.” The need to share information has been identified by seven of the nine combatant commands in their Integrated Priority Lists (IPLs). The Department of Defense lacks an information sharing strategy to guide the transition from today’s information sharing paradigm to a net-centric paradigm. Information sharing today occurs via interconnected physical networks separated by classification, whereas information sharing in a net-centric paradigm needs to be based upon classification and role-based access. Data strategy efforts enabling COIs, cross CDSs, and KM capabilities enabling secure information sharing with Joint, multinational, interagency, state, local and first responder mission partners are inadequate to mission needs (CJCS 6285.01, 2006.)

CENTRIXS-M is not intended to be a Family of Systems (FoS) or Systems of Systems (SoS), but rather an interim solution to achieving coalition communications until such time as a FoS or SoS is identified. However, CENTRIXS is the current DoD multinational (coalition, allied, bilateral and multinational) information sharing portion of the GIG. With the CENTRIXS-M BLK II/I variant scheduled to reach Full Operational

Capability (FOC) in FY2018 we are still a long way from identifying an overarching SoS for coalition communications. However, there are currently three operational Multinational Information Sharing (MNIS) systems including CENTRIXS.

The second MNIS system, Griffin, is a framework to provide a permanent, multi-nationally-developed, managed, and resourced capability that enables the exchange of information between the classified networks of participating nations at the SECRET level. Griffin encompasses necessary infrastructure, connectivity, applications, services, management, and governance. The reach of Griffin is dependent on the reach of each nation's classified network to its lower levels of command. All nations that participate on Griffin contribute, materially and in-kind, to the development, operation, and management of the capability. The Griffin infrastructure is a network of guards allowing e-mail between national systems.

The Combined Federated Battle Laboratory Network (CFBLNet) is a distributed Wide Area Network (WAN) used by the Combined Communications Electronics Board (CCEB) and NATO to conduct coalition communication experiments. The CCEB is a five nation joint military communications-electronics organization whose mission is the coordination of any Communications-Electronics (C-E) matters referred by a member nation. The CCEB member nations are Australia, Canada, New Zealand, the United Kingdom and the United States. A similar organization, Multinational Interoperability Council (MIC) is an operator led forum, which identifies interoperability issues and articulates actions, which contribute to more effective coalition operations. The member nations of the MIC are Australia, Canada, France, Germany, Italy, the United Kingdom and the United States. Although New Zealand and NATO Allied Command Transformation (ACT) are not members of the MIC they enjoy official observer status.

Therefore, of the three MNIS program listed only CENTRIXS and Griffin are actually operational MNIS systems while direct support for testing is provided by the CFBLNET until broader Net-Centric Enterprises Services (NCES) and GIG compliant approach to MNIS is developed. This interim process is established to match user requirements for operations and maintenance support of existing systems with programmed funding. CENTRIXS, Griffin, and CFBLNET provide proven operational and research, development, testing & evaluation (RDT&E) capabilities and services that must be sustained to support current and anticipated war fighter needs. The MNIS current operational systems will continue to provide capabilities to combatant commands, Services, and agencies until the objective MNIS replaces or consolidates an operational capability equal to or greater than the capability provided by the current operational system. The operations and sustainment support for MNIS current operational systems will evolve to a Services Based Sustainment (SBS) concept integrated into the Defense Information Systems (CJCSINST 6285.01, 2006.)

New, increased capabilities designed to support valid information sharing requirements will be managed on a case-by-case urgency-of-need basis through the Joint Urgent Operational Need (JUON) process as an exception to policy. During the interim period until the objective MNIS program is established, current operational system sustainment requirements are managed by this instruction. As the DoD Executive Agent (EA) for MNIS formally establishes the objective MNIS program, DoD EA for MNIS will establish and manage the associated longer-term objective program requirements process. Following the migration of current operational system capabilities to complete oversight by the DoD EA for MNIS and the DISA MNIS Joint Program Office (JPO), the DoD EA for MNIS will manage the process for all objective program requirements procedures.

It is clear the future coalition communications requirement will continue to increase while we attempt to cover gaps in our capabilities. The Joint Staff/J-6 will continue to gather international requirement considerations related to the CCEB, MIC, North Atlantic Treaty Organization (NATO), North American Air Defense (NORAD) Command, and United Nations Command (UNC) partnerships participating in CENTRIXS, Griffin, and CFBLNET. USEUCOM normally collects NATO requirements. Allied nations, coalition partners, and other participating nations that are not formal members of CCEB, MIC, NATO, NORAD and UNC may submit requirements through combatant command sponsors to Joint Staff/J-6. CENTRIXS is filling a critical capabilities gap in our C4I architecture, and will continue to be our primary means of coalition communications through FY2018.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. SUMMARY DISCUSSION

The United States is an undisputed global leader and pioneer in developing Network Enabled Capabilities. The Network Centric Warfare (NCW) program is at the heart of the U.S. transformation strategy, as defined in the Joint Vision 2020, and CENTRIXS is a capability that can make this transformation strategy a reality. According to Former Deputy Secretary of Defense Paul Wolfowitz, our (U.S.) ability to leverage the power of information and networks will be key to our success." By 2012, NCW should reach full capability, which will include a single network of sensors, deciders and shooters; IP addressable warriors, weapons and sensors; and commanders' shared awareness and knowledge.

The GIG system in conjunction with CENTRIXS will be the largest information network in the world and the key element of U.S. network-centric capabilities. Built based on commercial technologies, it will provide processing, storage, management, and transport of information to support all DoD, national security, and related intelligence community missions and functions. GIG capabilities will be available from all operating locations: bases, posts, camps, stations, facilities, mobile platforms, and deployed sites. The GIG will interface with allied, coalition, and non-GIG systems. Next-generation satellites will provide massive amounts of real-time information to platforms and weapon systems deployed on the tactical edge. Every square meter of the globe will have its own IP address, thus enabling effective tracking of all actors on the battlefield. The $34 billion program should be completed by 2011 (DoD PEO C4I, 2006.) Thanks to the GIG and CENTRIXS, deployed American soldiers will no longer be at the mercy of someone remote from the fight determining what information they need. CENTRIXS is at the heart of coalition communications and will continue to develop as the need for ease of information sharing becomes more and more critical throughout the world.

B. RECOMMENDATIONS FOR FURTHER RESEARCH

Information sharing is an ongoing problem that continues to stifle effective and efficient military operations. As seen in Iraq, Afghanistan, and other theaters, interagency and coalition partners all have a problem with information sharing. Part of the problem stems from cross-domain solutions, which are being worked very hard. The result is a so-called "sneaker net," in which information is put into a computer that is then carried to those who need it. Needless to say, this is not what should be expected out of the largest, most powerful, and most digitized military on earth. Trust, not technology, is at the core of the problem. Currently, CENTRIXS connects over thirty countries within Europe, Africa, and the Middle East, yet most information sharing agreements are bilateral, resulting in all sorts of communication breakdowns. For example, information comes in sent by Romanian troops to U.S. officials who in turn want to share it with British commanders. The problem is that cross-domain solutions keep popping up and have never been certified from an information assurance standpoint. The reliability of the solution is ultimately unknown. As a result, senior coalition members in Afghanistan and Iraq do not have access to DoD secret networks.

To address the issue, a new identity-based, information assurance network is needed. This network would let the software decide who gets what. This solution would mimic a similar effort, DoD's Cross Domain Collaborative Information Environment, which is being managed by U.S. Joint Forces Command and recently completed the first phase of the National Security Agency's Certification Test and Evaluation process.

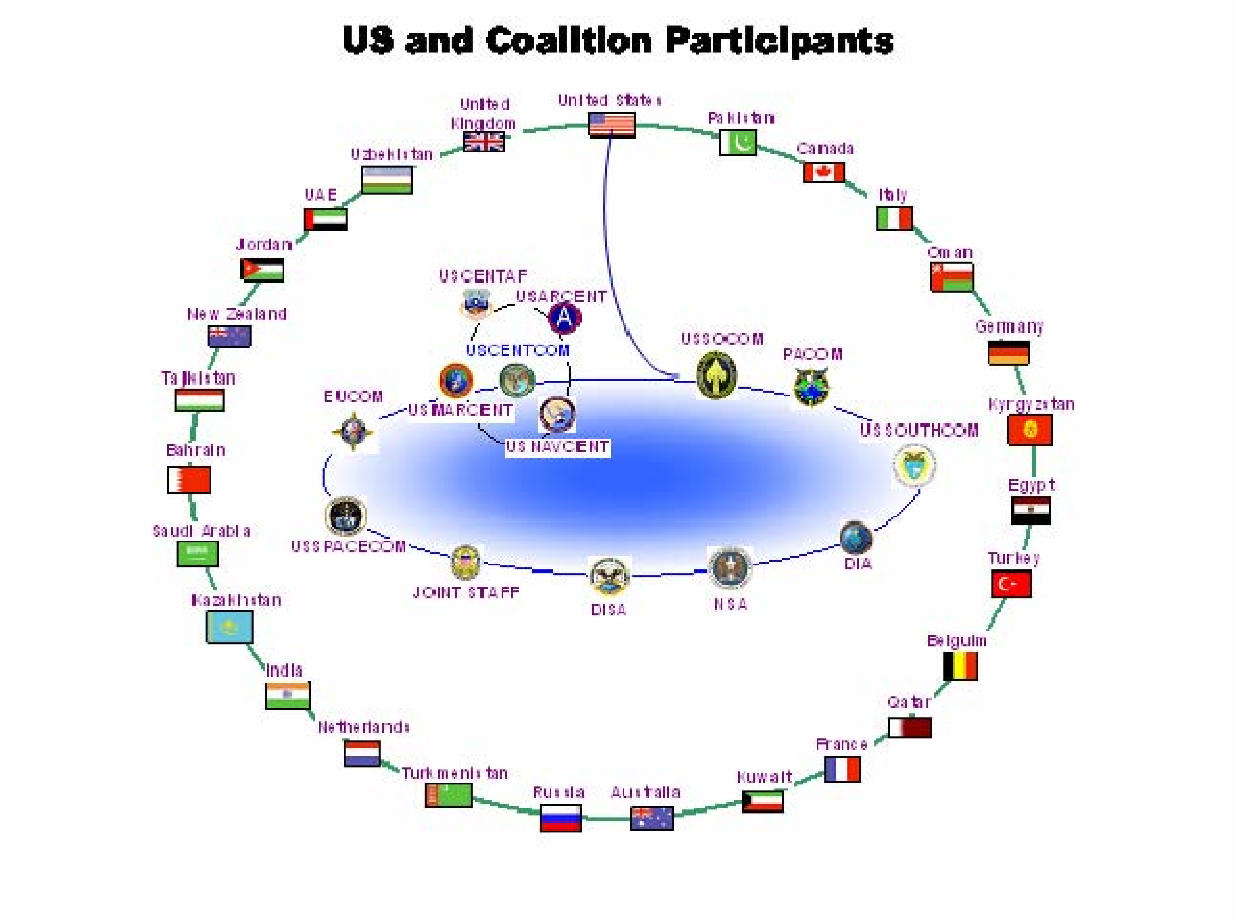
Another problem is that currently CENTRIXS connectivity to GIG/DISN access and other U.S. classified resources is tremendously limited. Information can be moved between the U.S. secret environment and the coalition environment through appropriate Content Filters (e.g., Radiant Mercury)._ Currently, it is important to point out that these options for "reach-back" connectivity to the National Communication and Information System are available only to U.S. users of CENTRIXS networks. Non-U.S. users currently access information resources through directly connected workstations or LANs, employing the information services provided by the particular CENTRIXS enclave(s) to which they are connected. It is also worth noting that some of the content-filtering/guard technologies, like Radiant Mercury12, are based on commercially unavailable operating systems.

The releasability of these capabilities will influence the degree of connectivity between CENTRIXS and NATO/National systems, which will affect the richness of non-U.S. contributions to CENTRIXS-based information exchange/sharing. Realizations of Network-Centric Operations/Network-Enabled Capability in a coalition environment will depend on the elimination of "air-gapping" solutions to the question of information exchange/sharing. Network-level and system-level interconnection of non-U.S. systems to CENTRIXS will be required, not just extension of the CENTRIXS component network VPNs into coalition partners facilities. In the future, access via the national networks of coalition nations and access to the information systems and services on the national networks could be facilitated through a Regional Gateway, as defined under CENTRIXS. This architecture solution proposed for the CENTRIXS Regional Gateway closely resembles the NATO Information Exchange Gateway, NATO's approach to information exchange/sharing between NATO, its Member Nations, and NATO-led Coalitions.

As the CENTRIXS program manager for CENTRIXS-GCTF, the third author of this document has tested this solution with the cooperation of Sun Microsystems in the Afghanistan AOR. Unfortunately, DISA releasability guidelines prohibit implementation of this initiative over the full family of CENTRIXS enclaves.

As challenging as it was to build an infrastructure to support U.S. forces, an even more daunting task is the incorporation of the various coalition partners who arrive at a Combined-Joint Operation expecting to be fully incorporated into the CENTRIXS architecture. From a political perspective, planners can count on the coalition partnership containing a new set of members for every operation for the next contingency. Each of these members will have entirely different sets of communications equipment that will assuredly not be compatible with what is being prescribed as the CENTRIXS standard. The answer is to source additional funds to the CENTRIXS program manager to put into service a FAK that can be acquired by participating counties to connect to the CENTRIXS network where interface is required. This FAK will be modular, adaptable, scalable, secure end-to-end and built entirely from commercial off-the-shelf technologies. The FAK will be designed with the intent of increasing the CENTRIXS forward presence, connecting all participating countries, and extending the network to austere locations. This initiative would alleviate the issue of countries with scarce resources not being able to fully participating in coalition efforts due to inadequate or incompatible equipment.

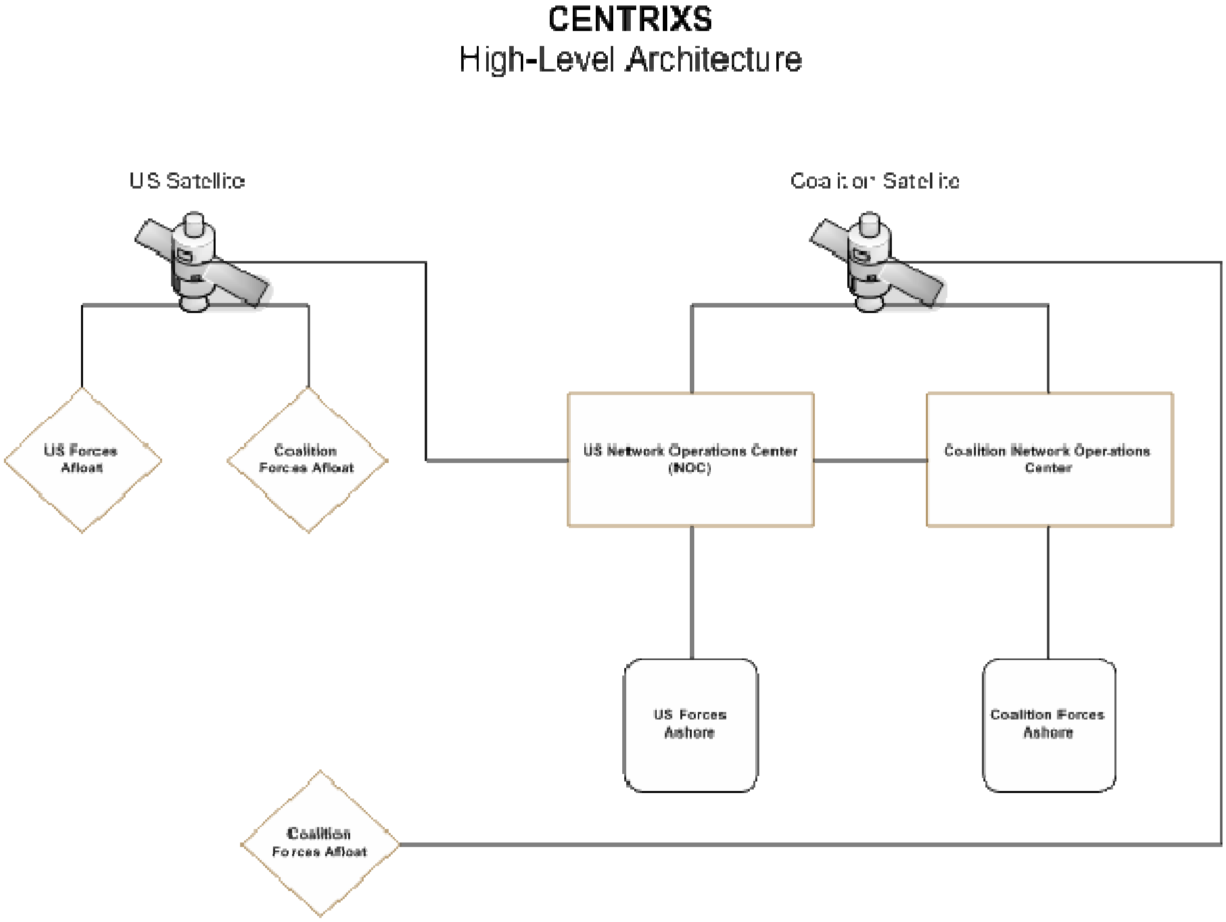
APPENDIX A. EXAMPLE OF U.S. AND COALITION STRATEGIC INTEROPERABILITY



This diagram depicts U.S. and Coalition Strategic Interoperability and illustrates supporting commands and agencies at the operational level (USCENTCOM, 34, 2004.)

THIS PAGE INTENTIONALLY LEFT BLANK

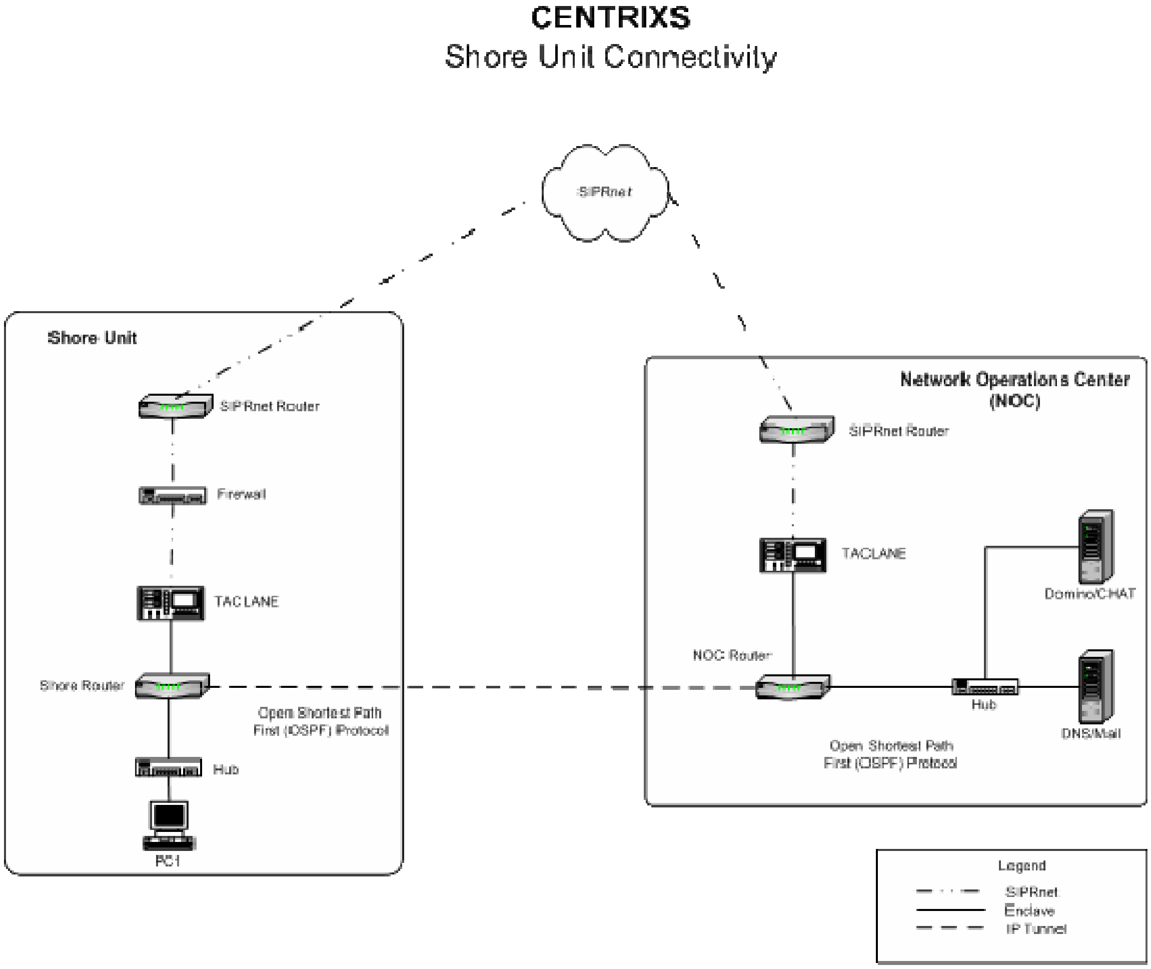
APPENDIX B. CENTRIXS HIGH-LEVEL ARCHITECTURE



This diagram depicts the CENTRIXS High-Level Architecture, and illustrates the network connectivity installed on surface ships and at the Navy's Regional Network Operations Centers (USCENTCOM, 45, 2004.)

THIS PAGE INTENTIONALLY LEFT BLANK

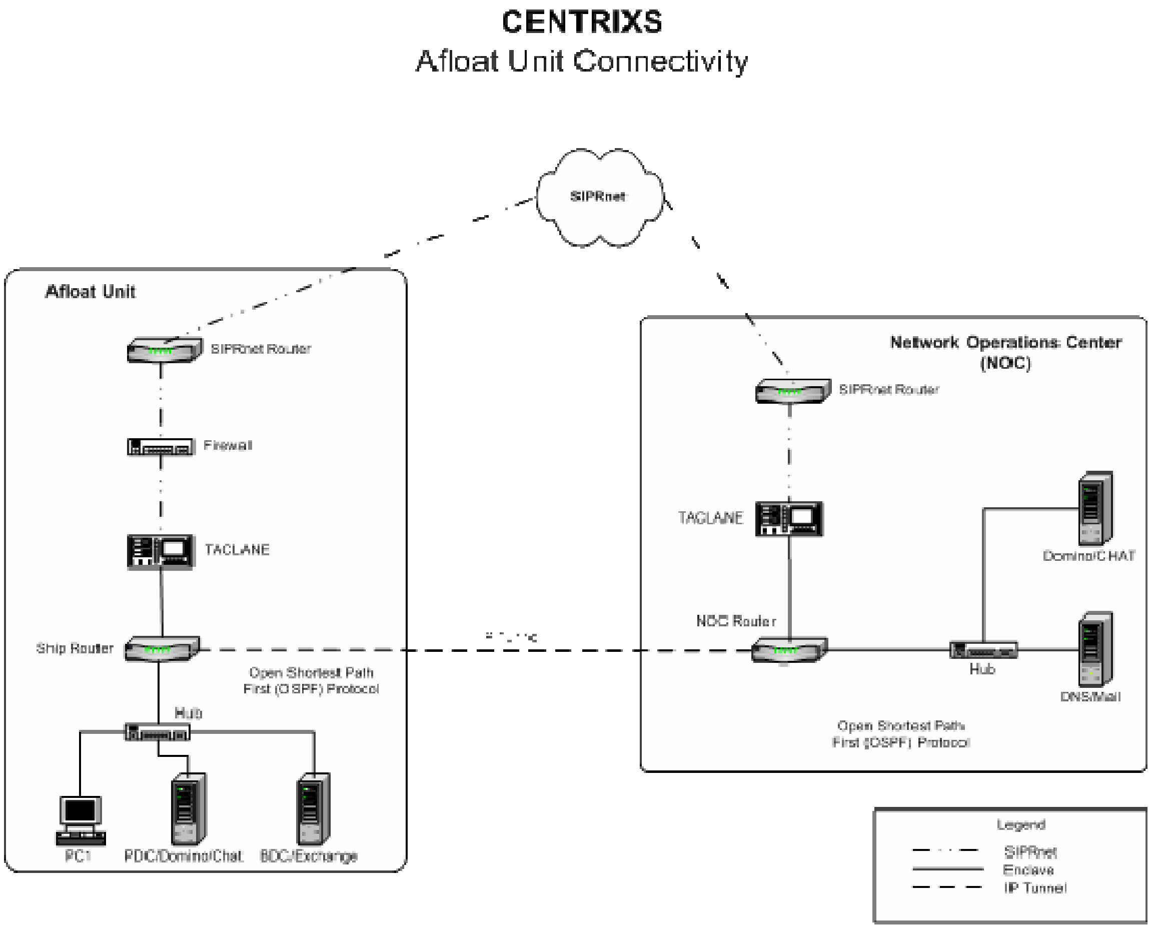
APPENDIX C. CENTRIXS SHORE UNIT CONNECTIVITY



This diagram illustrates the notional architecture for CENTRIXS shore unit connectivity.

THIS PAGE INTENTIONALLY LEFT BLANK

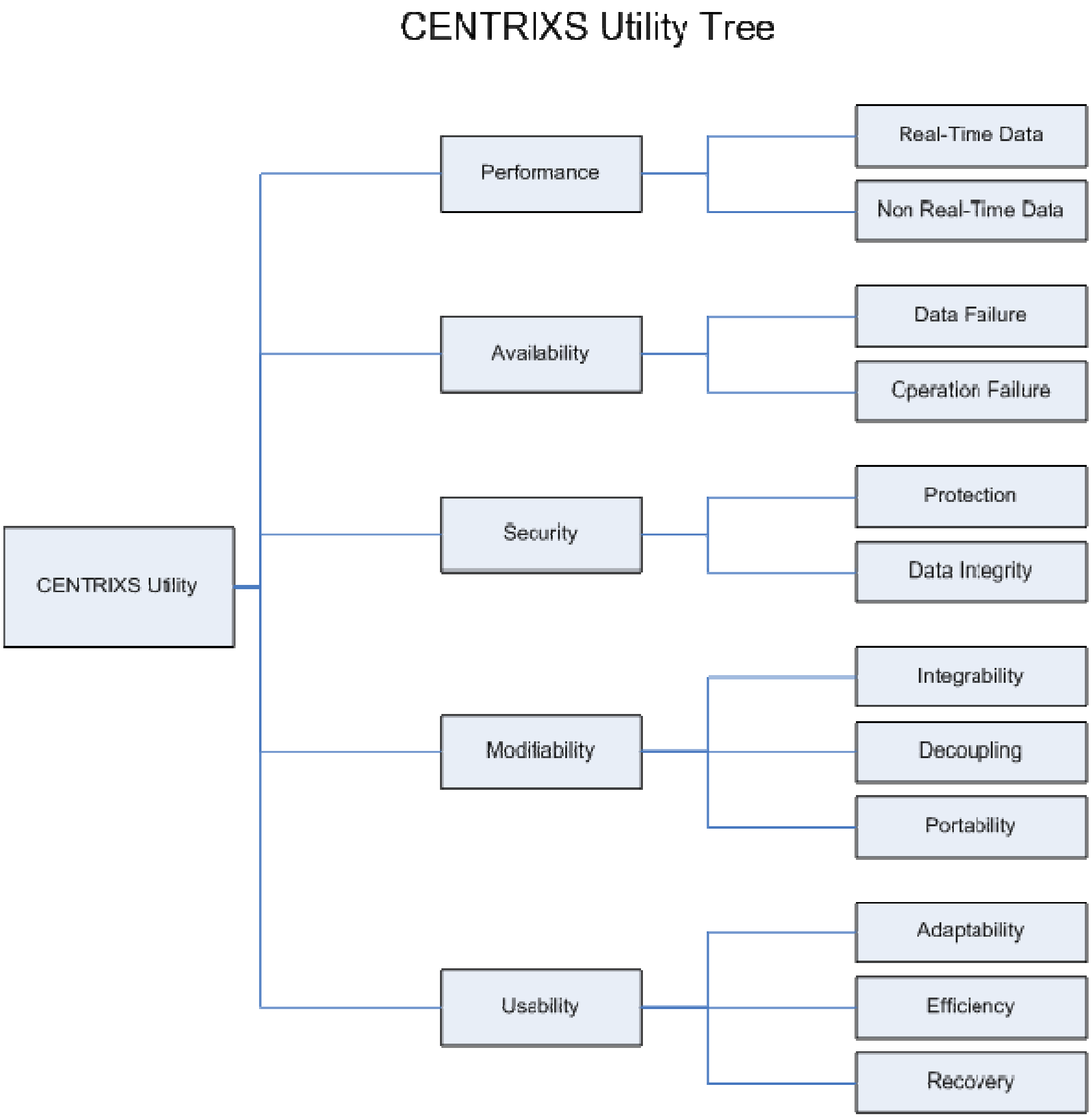
APPENDIX D. CENTRIXS AFLOAT UNIT CONNECTIVITY



This diagram illustrates the notional architecture for CENTRIXS afloat unit connectivity.

THIS PAGE INTENTIONALLY LEFT BLANK

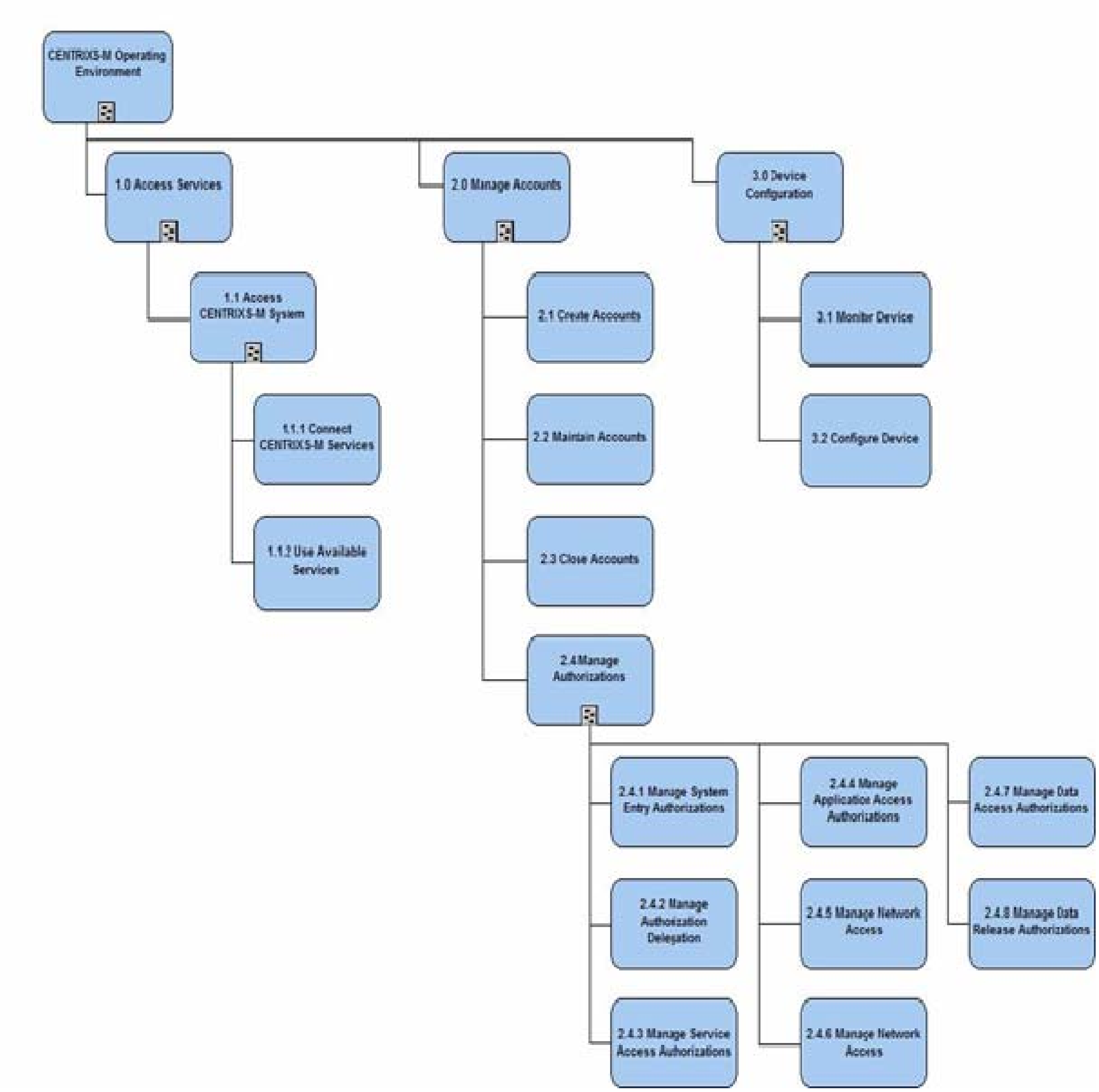
APPENDIX E. CENTRIXS UTILITY TREE



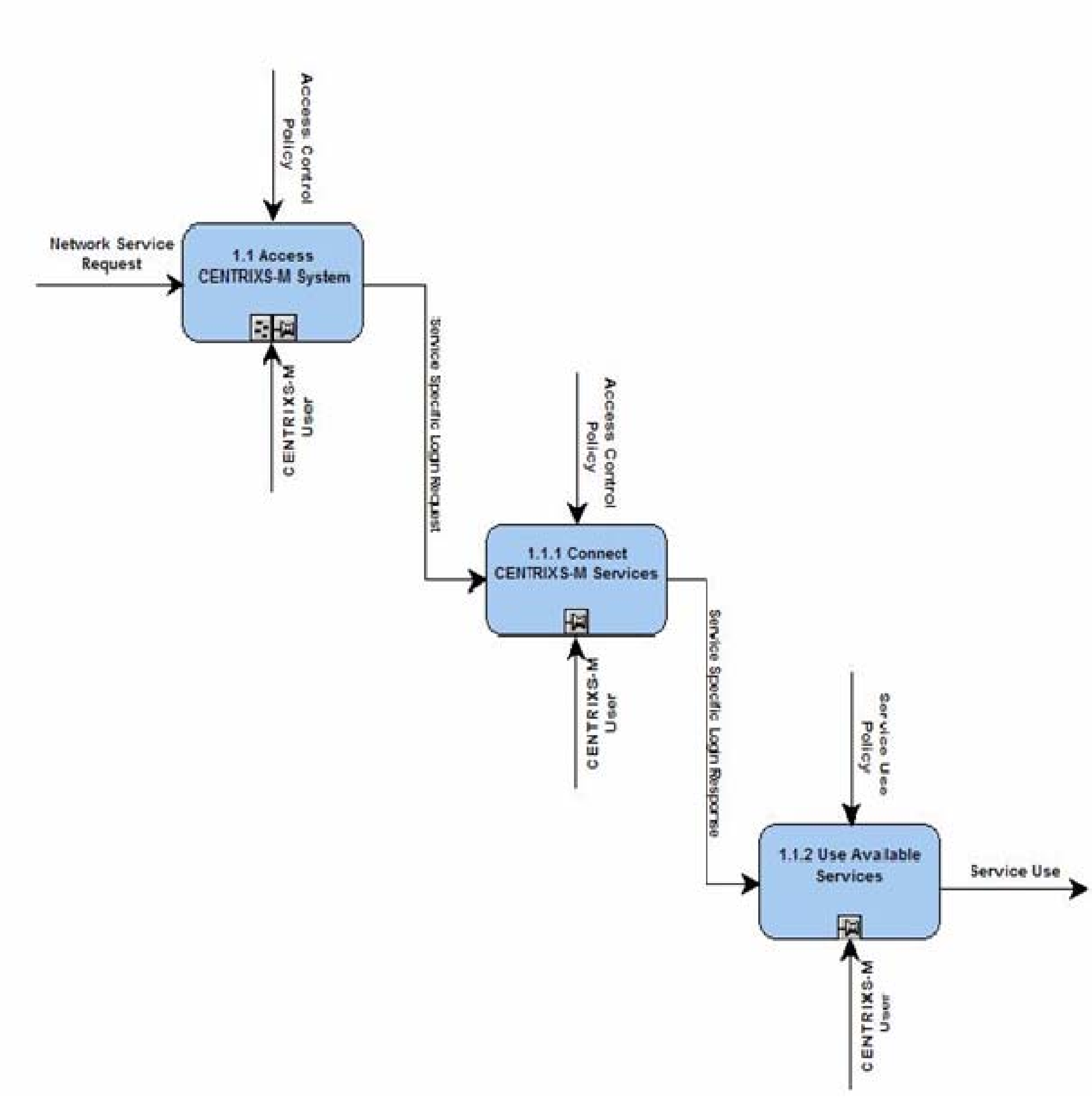
The CENTRIXS Utility Tree is a detailed listing of the functional requirements and key quality attributes of the CENTRIXS network.

THIS PAGE INTENTIONALLY LEFT BLANK

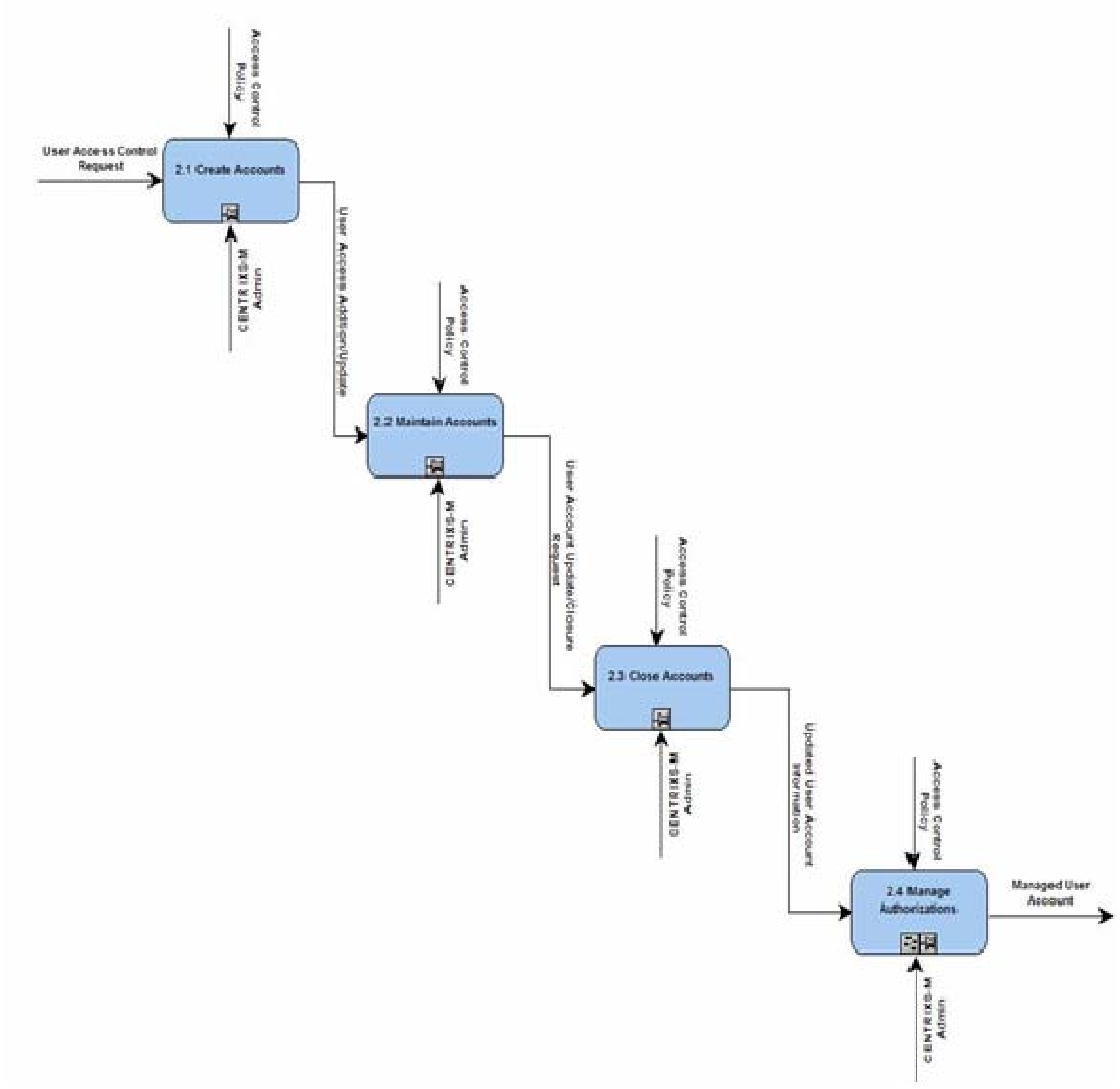
APPENDIX F. OPERATIONAL ACTIVITY MODEL OVERVIEW


CENTRIXS-M Operating Environment
1.0 Access Services
2.0 Manage Accounts
3.0 Device Configuration
1.1 Access CENTRIXS-M System
1.1.1 Connect CENTRIXS-M Services
1.1.2 Use Available Services
2.1 Create Accounts
2.2 Maintain Accounts
2.3 Close Accounts
2.4 Manage Authorizations
3.1 Monitor Device
3.2 Configure Device
2.4.1 Manage System Entry Authorizations
2.4.2 Manage Authorization Delegation
2.4.3 Manage Service Access Auhorizations
2.4.4 Manage Application Access Authorizations
2.4.5 Manage Network Access
2.4.6 Manage Network Access
2.4.7 Manage Data Access Authorizations
2.4.8 Manage Data Release Authorizations

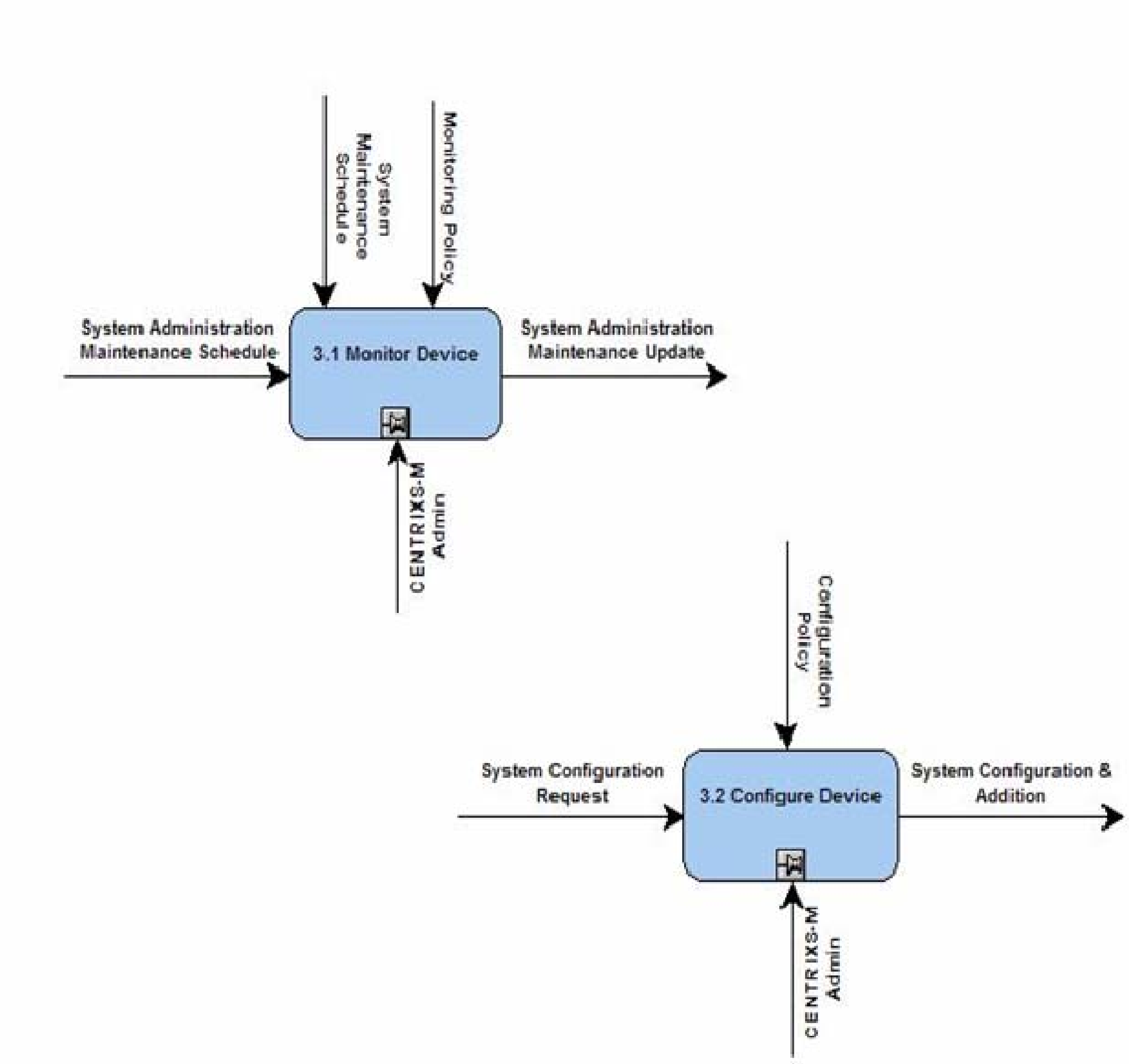
The Operational Activity Model graphically illustrates the "how" (operational activities) and "what" (Information Exchanges) data elements of a given architecture at the owner's level of detail (From: Ching, 2007.)


Access Control Policy
Network Service Request
1.1 Access CENTRIXS-M System
CENTRIXS-M User
Service Specific Login Request
Access Control Policy
1.1.1 Connect CENTRIXS-M Services
CENTRIXS-M User
Service Specific Login Response
Service Use Policy
1.1.2 Use Available Services
Service Use
CENTRIXS-M User

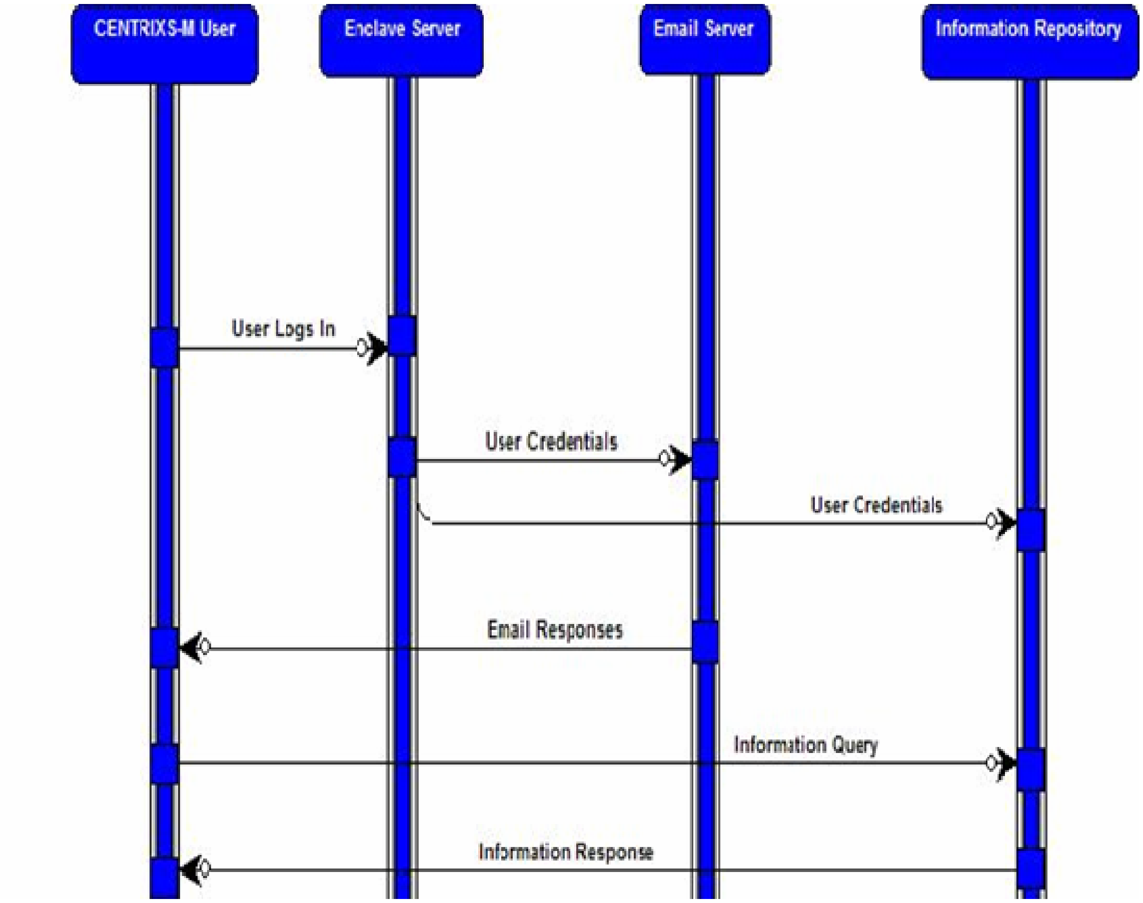
This diagram of the Operational Activity Model shows operators access one or more of the network services via network service requests. After accessing any network service(s), operators may logout or access other services. Operator session will terminate upon operator logout (From: Ching, 2007.)



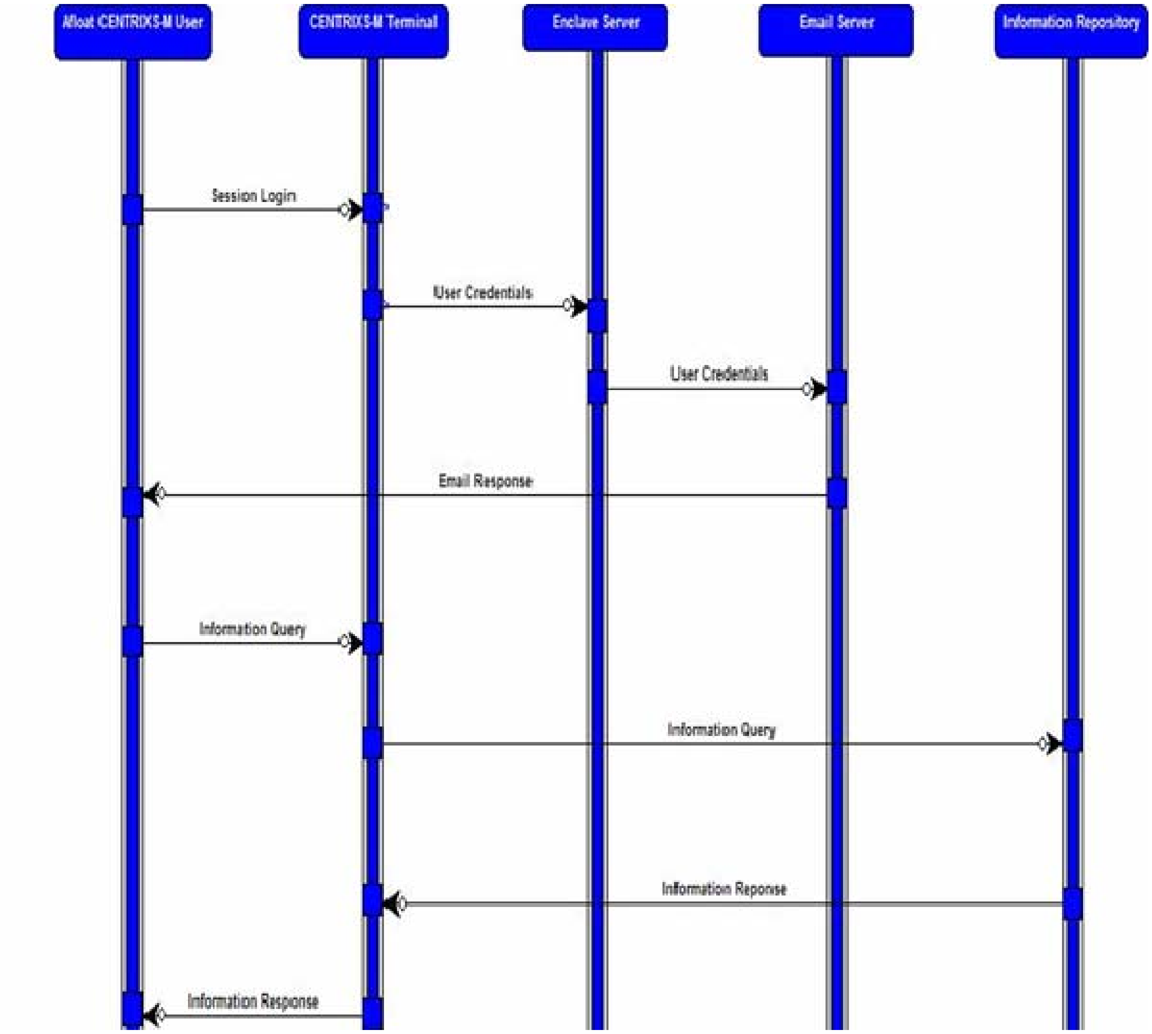
This diagram of the Operational Activity Model represents the explicit IA functionality provided by the CENTRIXS. IA functionality that exists as a support function implicit to other functionality is not included in this activity model (From: Ching, 2007.)


System Maintenance Schedule
Monitoring Policy
System Administration Maintenance Schedule
3.1 Monitor Device
System Administration Maintenance Update
CENTRIXS-M Admin
Configuration Policy
System Configuration Request
3.2 Configure Device
System Configuration & Addition
CENTRIXS-M Admin

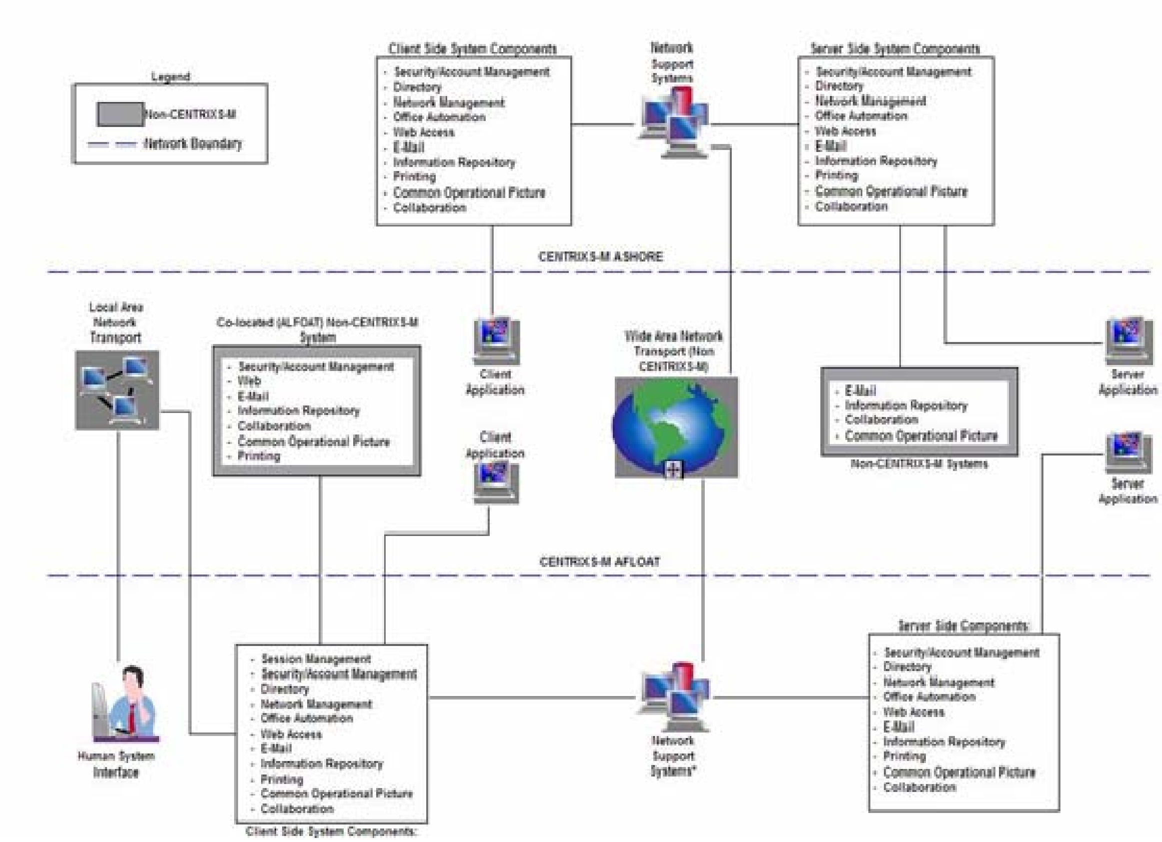
This diagram of the Operational Activity Model depicts the process flow for both system maintenance, and configuration requests annotating the impact of policy on operations (From: Ching, 2007.)



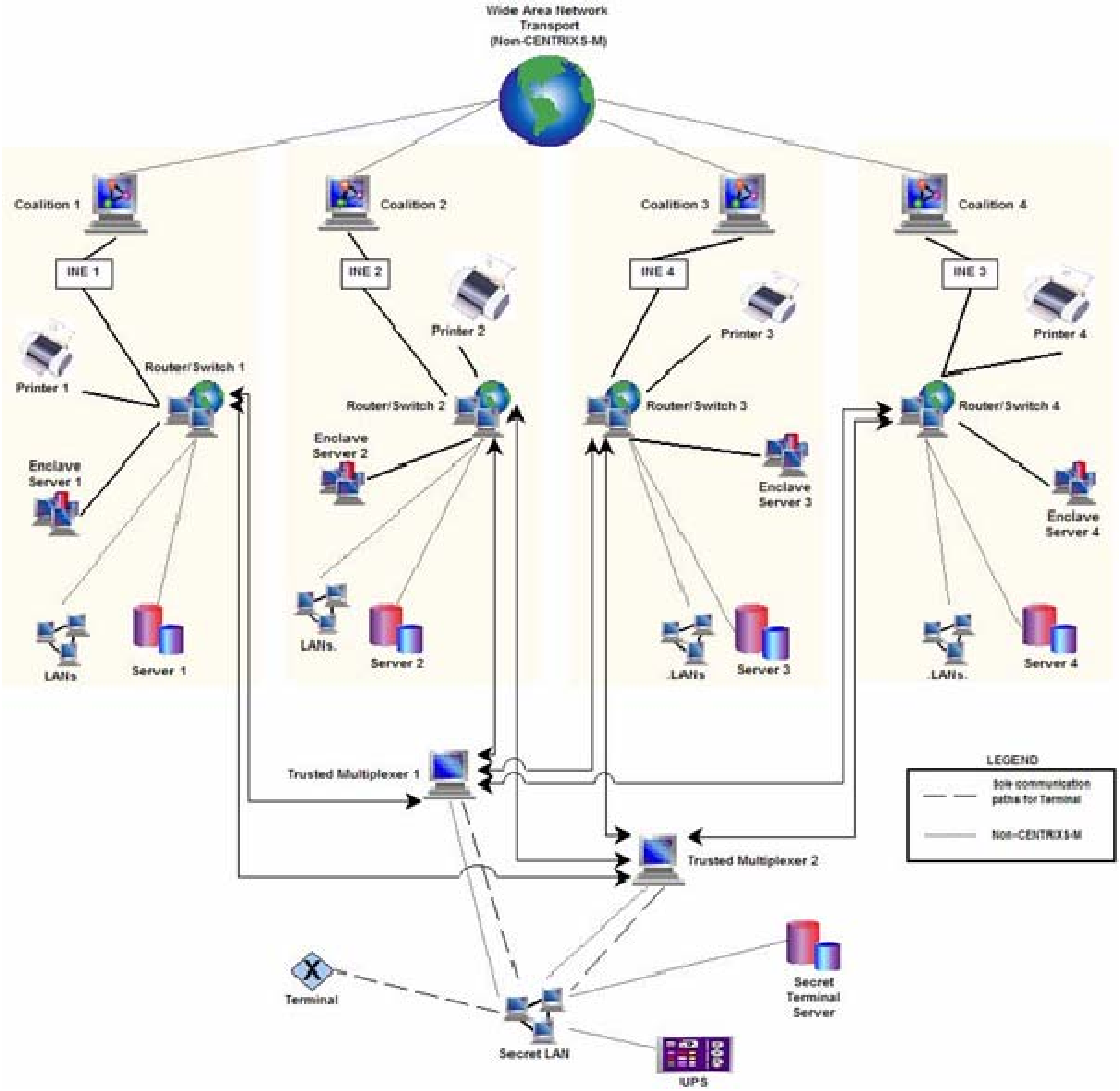
This diagram of the Operational Activity Model describes the sequencing of activities in the OV-5 model. Events may also be referred to as inputs, transactions or triggers. Timing of these events is not critical for any of the CENTRIXS functionality, because there are certain time requirements for completion of individual information exchanges (From: Ching, 2007.)



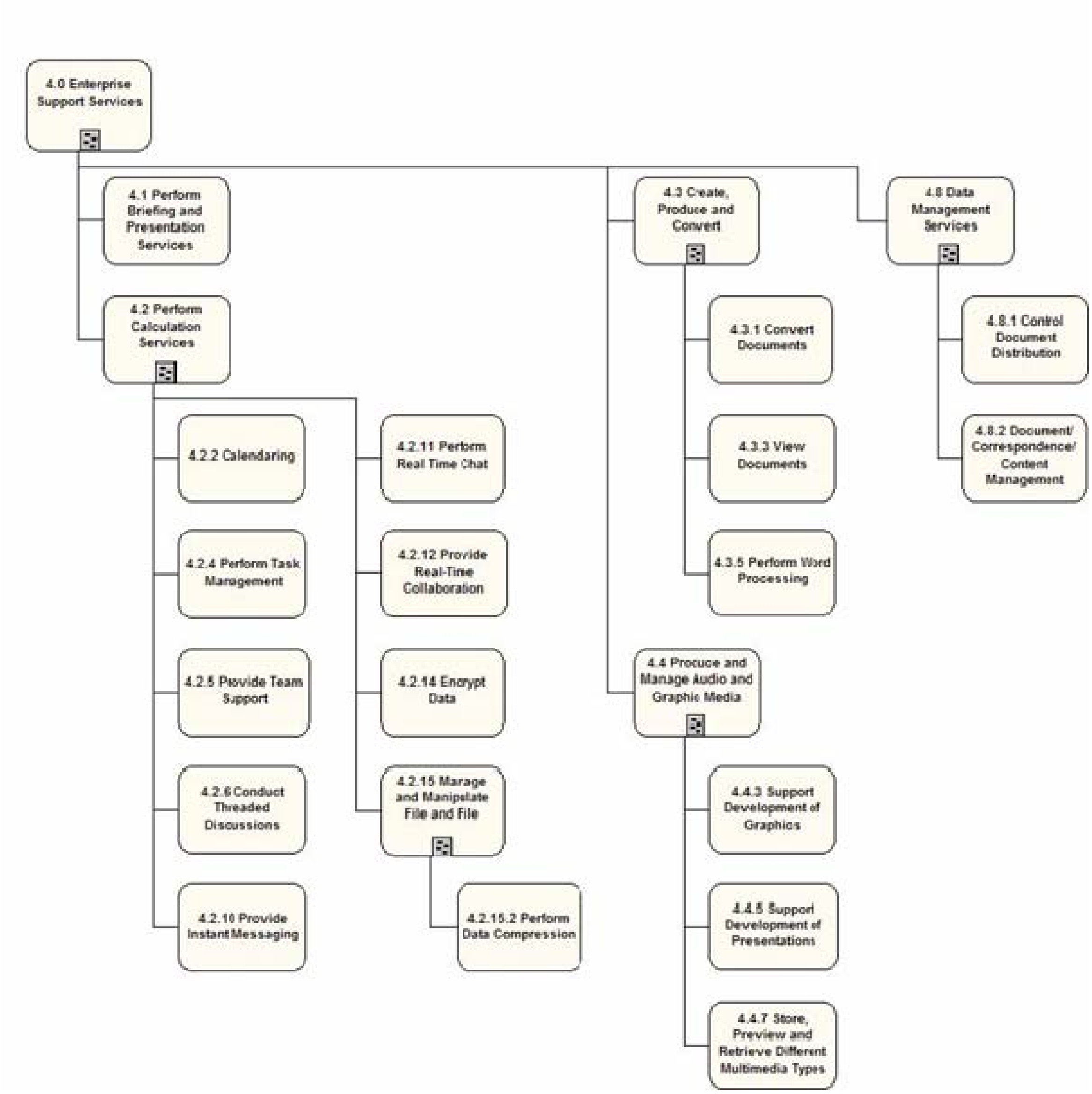
This diagram of the Operational Activity Model shows that the security administrative operator may create, modify, or delete operator accounts. The non-system or security administrative operator logs into the network via a session login and then logs into an enclave to access network services. Lacking administrative or security privileges, the operator may only access the network services. The operator may return to access other services as often as desired until the decision is made to logout (From: Ching, 2007.)



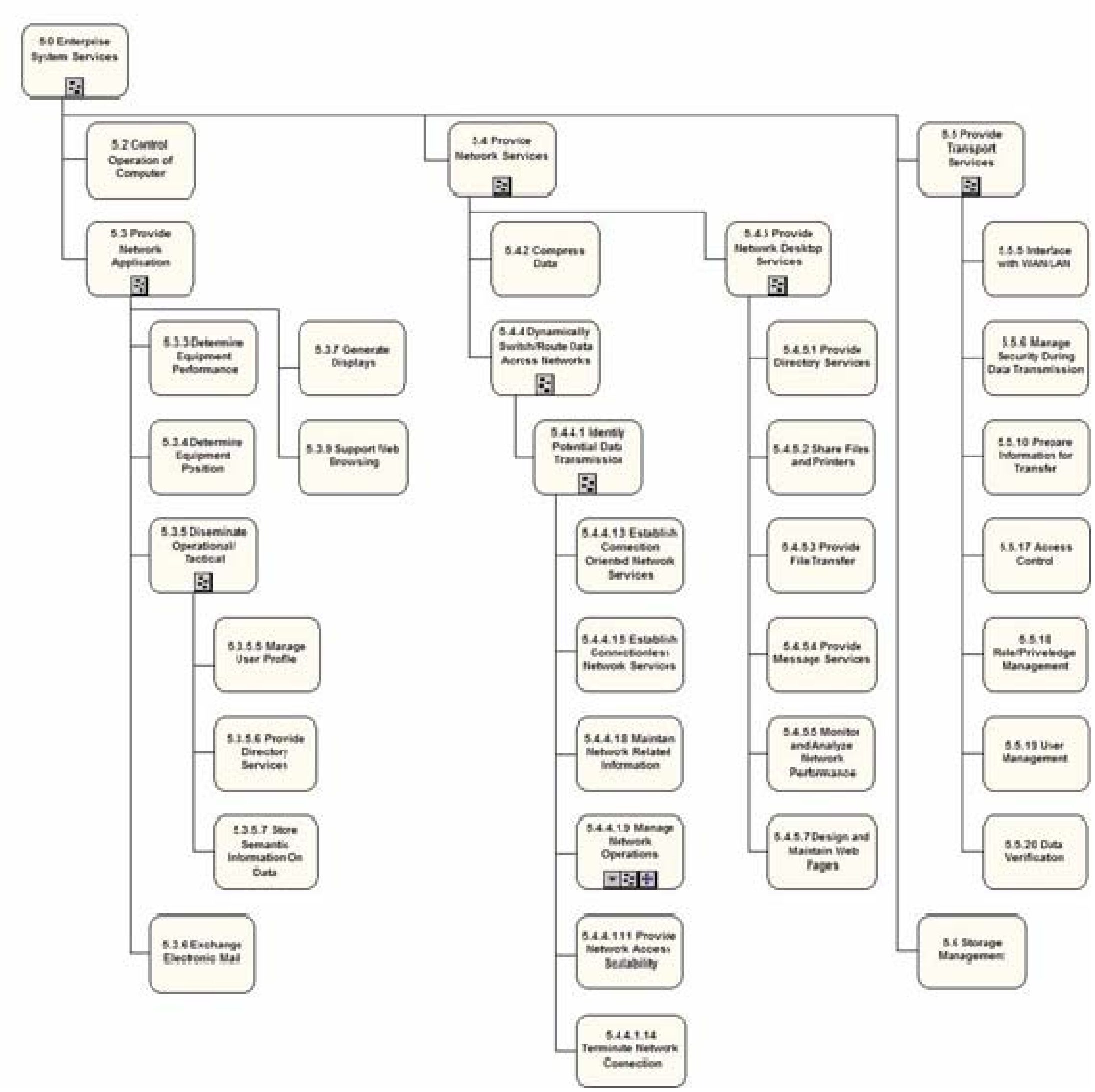
This diagram of the Operational Activity Model is a System Interface Diagram, which shows the relationships between CENTRIXS users (From: Bayer, 2007.)



This diagram of the Operational Activity Model provides a system communication description. It illustrates how different CENTRIXS nodes communicate (From: Ching, 2007.)

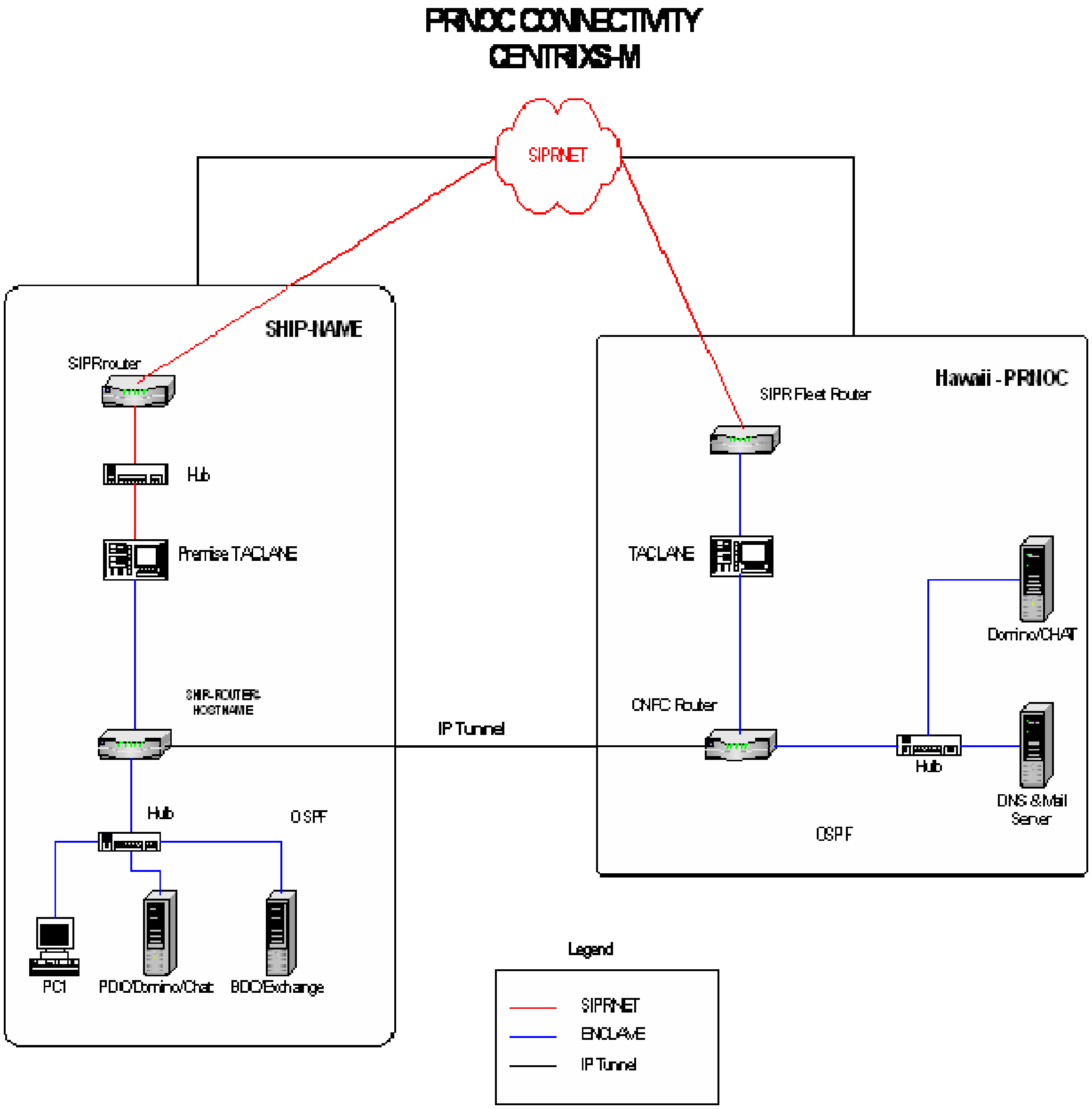

4.0 Enterprise Support Services
4.1 Perform Briefing and Presentation Services
4.2 Perform Calculation Services
4.2.2 Calendaring
4.2.4 Perform Task Management
4.2.5 Provide Team Support
4.2.6 Conduct Threaded Discussions
4.2.10 Provide Instant Messaging
4.2.11 Perform Real Time Chat
4.2.12 Provide Real-Tine Collaboration
4.2.14 Encrypt Data
4.2.15 Marage and Manipslate File and File
4.2.15.2 Perform Data Compression
4.3 Create, Produce and Convert
4.3.1 Convert Documents
4.3.3 View Documents
4.3.5 Perform Word Processing
4.4 Procuce and Manage Audio and Graphic Media
4.4.3 Support Development of Graphics
4.4.5 Support Development of Presentations
4.4.7 Store, Preview and Retrieve Different Multimedia Types
4.8 Data Management Services
4.8.1 Control Document Distribution
4.8.2 Document/ Correspondence/ Content Management

This diagram of the Operational Activity Model shows the relationships between the Enterprise Support Services (From: Ching, 2007)

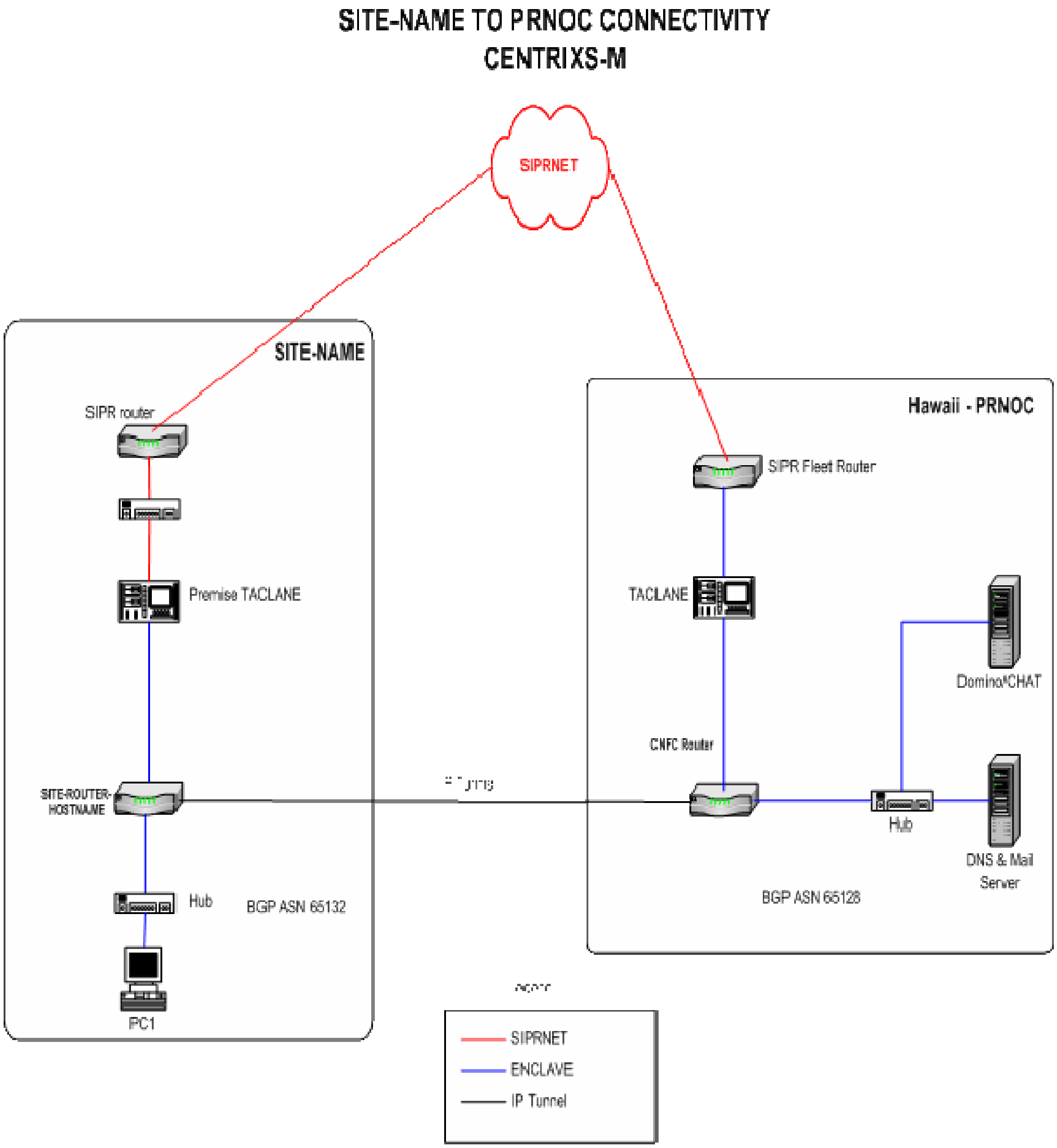

5.0 Enterprise System Services
5.2 Control Operation of Computer
5.3 Provide Network Application
5.3.3 Determine Equipment Peformance
5.3.7 Generate Displays
5.3.4 Determine Equipment Position
5.3.9 Support Web Browsing
5.3.5 Diseminate Operational/ Tactical
5.3.5.5 Manage User Profile
5.3.5.6 Provide Directory Services
5.3.5.7 Store Semantic Information On Data
5.3.6 Exchange Electronic Mail
5.4 Provide Network Services
5.4.2 Compress Data
5.4.4 Dynamically Switch/Route Data Across Networks
5.4.4.1 Identify Potential Data Transmission
5.4.4.1.3 Establish Connection Oriented Network Services
5.4.4.1.5 Establish Connectionless Network Services
5.4.4.1.8 Maintain Network Related Information
5.4.4.1.9 Manage Network Operations
5.4.4.1.11 Provide Network Access Scalability
5.4.4.1.14 Terminate Network Conection
5.4.5 Provide Network Desktop Services
5.4.5.1 Provide Directory Services
5.4.5.2 Share Files and Printers
5.4.5.3 Provide File Transfer
5.4.5.4 Provide Message Services
5.4.5.5 Monitor and Analyze Network Performance
5.4.5.7 Design and Maintain Web Pages
5.5 Provide Transport Services
5.5.5 Interface with WAN/LAN
5.5.6 Manage Security During Data Transmission
5.5.10 Prepare Information for Transfer
5.5.17 Access Control
5.5.18 Role/Priveledge Management
5.5.19 User Management
5.5.20 Data Verification
5.6 Storage Management

This diagram of the Operational Activity Model shows the relationships between the Enterprise System Services (From: Ching, 2007.)

APPENDIX G. TYPICAL PRNOC CONNECTIVITY



This diagram illustrates the way a typical PRNOC is set up for connectivity with a ship (From: Chang, 2007.)



This diagram illustrates the way a typical PRNOC is set up for connectivity to a particular land site (From: Chang, 2007.)

APPENDIX H. CENTRIXS NPS SURVEY DOCUMENTS

Naval Postgraduate School
Informed Consent Form

Introduction. You are invited to participate in a survey entitled CENTRIXS at NPS.

Procedures. This survey should take between 5 and 10 minutes to complete, and will be comprised of questions related to a CENTRIXS install here at NPS. No personal information will be used other than to evaluate the benefits of installing a CENTRIXS node on campus. Following the survey, you may be contacted personally based on your answers for further research.

Risks and Benefits. I understand that this survey does not involve greater than minimal risk and involves no known reasonably foreseeable risks or hazards greater than those encountered in everyday life. I have also been informed of any benefits to myself or to others that may reasonably be expected as a result of this research.

Compensation. I understand that no tangible compensation will be given. I understand that a copy of the research results will be available at the conclusion of the experiment via thesis documentation.

Confidentiality & Privacy Act. I understand that all records of this survey will be kept confidential and that my privacy will be safeguarded. No information will be publicly accessible which could identify me as a participant. I will not be identified in research forms/data bases. I understand that records of my participation will be maintained by NPS for three years, after which they will be destroyed.

Voluntary Nature of the Survey. I understand that my participation is strictly voluntary, and if I agree to participate, I am free to withdraw at any time without prejudice.

Points of Contact. I understand that if I have any questions or comments regarding this project upon the completion of my participation, I should contact the Principal Investigator, LtCol Karl D. Pfeiffer, USAF, Asst. Professor, 831-656-3635, kdpfeiff@nps.edu. Any other questions or concerns may be addressed to the IRB Chair, LT Brent Olde, 656-3807, baolde@nps.edu.

Statement of Consent. I have been provided with a full explanation of the purpose, procedures, and duration of my participation in this survey. I understand how my identification will be safeguarded and have had all my questions answered. I have been provided a copy of this form for my records and I agree to participate in this survey. I understand that by agreeing to participate in this research, I do not waive any of my legal rights. By clicking the button below, I agree to participate in the survey.

INSTITUTION REVIEW BOARD (IRB) APPLICATION

Application for Human Subjects Review	NPS IRB Number:
Principal Investigator(s): Co- PI(s)	LtCol Karl D. Pfeiffer, USAF, Asst. Professor, 831-656-3635 Capt Douglas A. Cook, Student, 831-241-0032 LT Bobby Patto, Student LT Pat Lancaster, Student
Title of Experiment:	

Approval Requested [X] New [ ] Renewal [ ] Amendment

Requested Level of Risk [ ] Exempt [X] Minimal [ ] More than Minimal
Justification:

Work to be done in (Site/Bldg/Rm) Survey via e-mail	Estimated number of days to complete: 1
Maximum number of subjects: 400	Estimated length of each subjects participation: 5-10 minutes

Special Populations that will be Used as Participants:

[ ] Subordinates [ ] Minors [ ] NPS Students [ ] Special Needs (e.g. Pregnant women)

Specify safeguards to avoid undue influence and protect subject's rights:
This survey will be sent to most faculty members. It is completely voluntary and will ask for no personal information.

Scientific Merit Review (Check all that apply)

[ ] This research is part of a funded project (Job Order Number:)

[X] This research is a student thesis (Attach a copy of the approved thesis proposal)

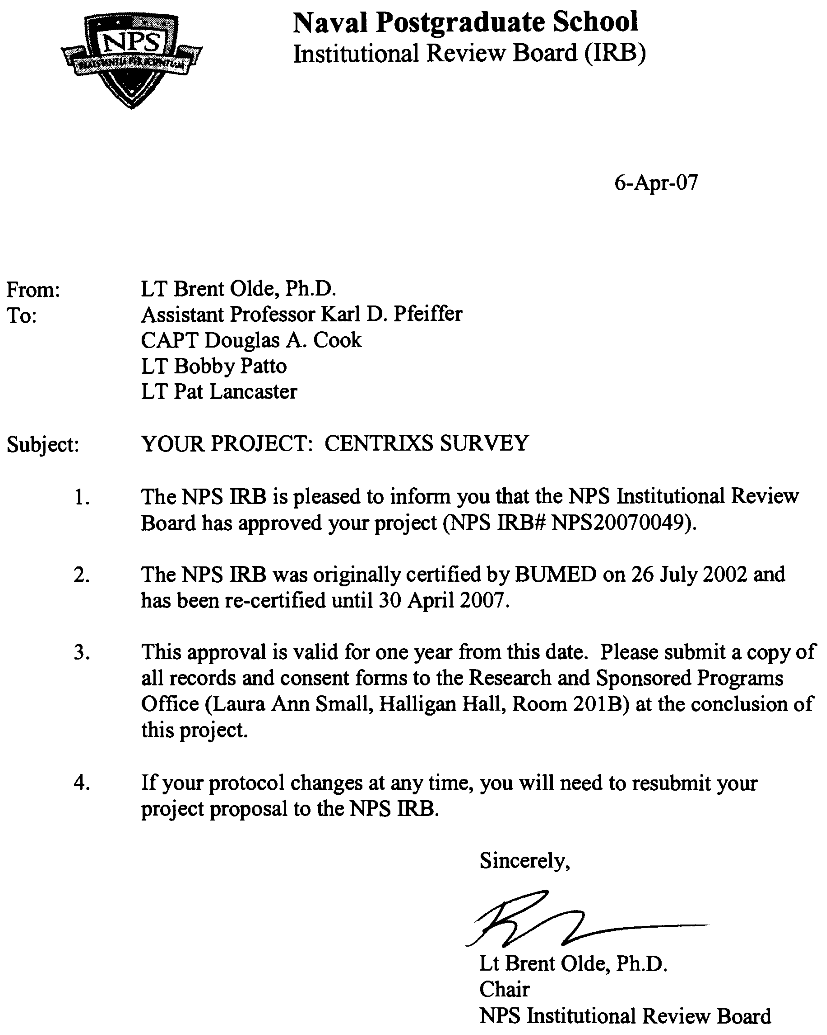
[ ] Other (Attach a complete research proposal - Dept. Chair must sign Application Cover Letter)

Outside Cooperating Investigators and Agencies: N/A
[ ] A copy of the cooperating institution's HSR decision is attached.

Description of Research: (attach an additional sheet if needed). This survey will be a 5-10 minute survey to the faculty in order to get an idea about how helpful it would be to have a CENTRIXS install here at NPS. It is completely voluntary, and will not ask for any personal information.

I have read and understand NPS policy on the Protection of Human Subjects. If there are any changes in any of the above information or any changes to the attached materials, I will suspend the experiment until I obtain new IRB approval.

SIGNATURE______________________________ DATE______________



Naval Postgraduate School
Institutional Review Board (IRB)

6-Apr-07

From: LT Brent Olde, Ph.D.
To: Assistant Professor Karl D. Pfeiffer
CAPT Douglas A. Cook
LT Bobby Patto
LT Pat Lancaster

Subject: YOUR PROJECT: CENTRIXS SURVEY

1. The NPS IRB is pleased to inform you that the NPS Institutional Review Board has approved your project (NPS IRB# NPS20070049).

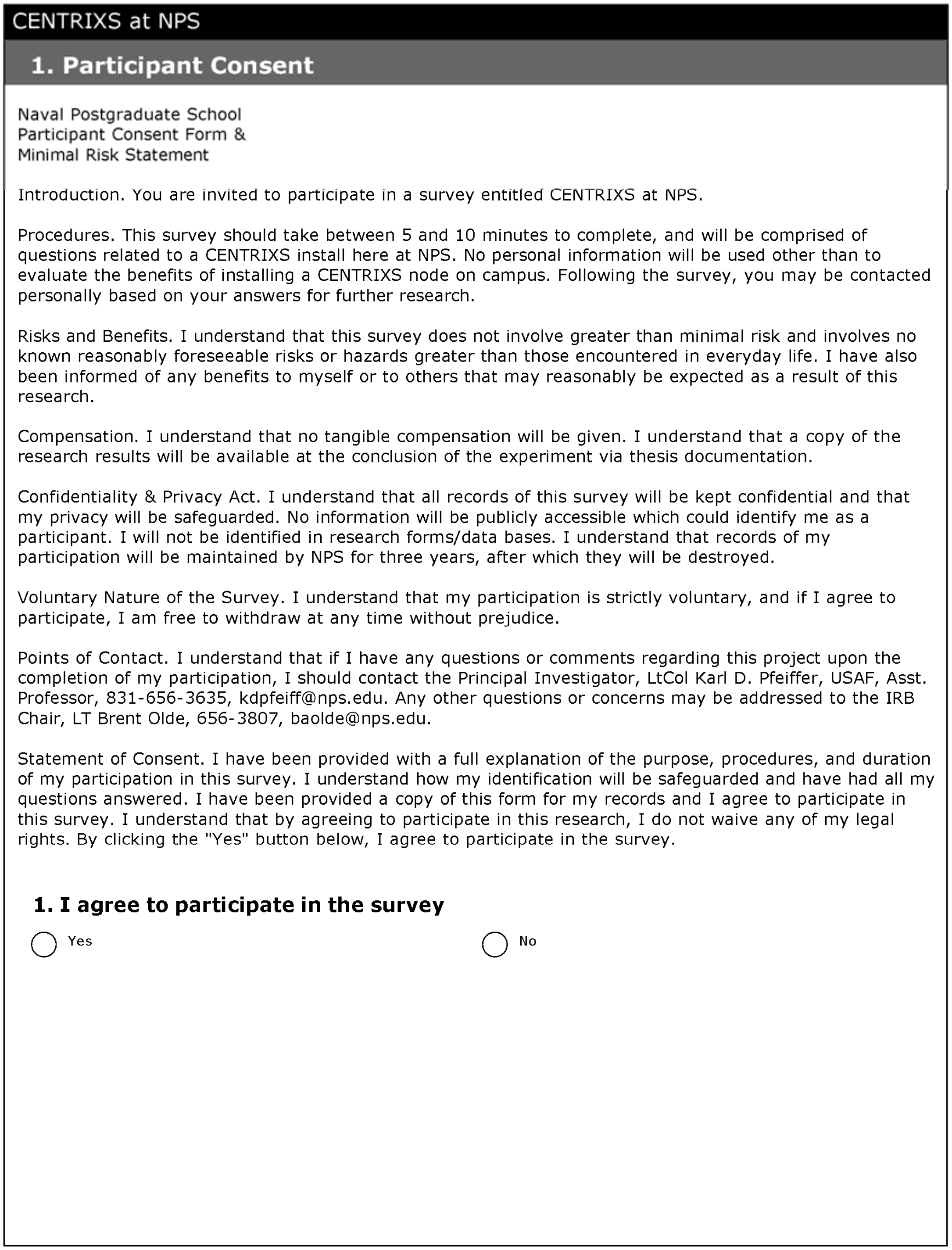
2. The NPS IRB was originally certified by BUMED on 26 July 2002 and has been re-certified until 30 April 2007.

3. This approval is valid for one year from this date. Please submit a copy of all records and consent forms to the Research and Sponsored Programs Office (Laura Ann Small, Halligan Hall, Room 201B) at the conclusion of this project.

4. If your protocol changes at any time, you will need to resubmit your project proposal to the NPS IRB.

Sincerely,

Lt Brent Olde, Ph.D.
Chair
NPS Institutional Review Board



CENTRIXS at NPS

1. Participant Consent

Naval Postgraduate School
Participant Consent Form &
Minimal Risk Statement

Introduction. You are invited to participate in a survey entitled CENTRIXS at NPS.

Procedures. This survey should take between 5 and 10 minutes to complete, and will be comprised of questions related to a CENTRIXS install here at NPS. No personal information will be used other than to evaluate the benefits of installing a CENTRIXS node on campus. Following the survey, you may be contacted personally based on your answers for further research.

Risks and Benefits. I understand that this survey does not involve greater than minimal risk and involves no known reasonably foreseeable risks or hazards greater than those encountered in everyday life. I have also been informed of any benefits to myself or to others that may reasonably be expected as a result of this research.

Compensation. I understand that no tangible compensation will be given. I understand that a copy of the research results will be available at the conclusion of the experiment via thesis documentation.

Confidentiality & Privacy Act. I understand that all records of this survey will be kept confidential and that my privacy will be safeguarded. No information will be publicly accessible which could identify me as a participant. I will not be identified in research forms/data bases. I understand that records of my participation will be maintained by NPS for three years, after which they will be destroyed.

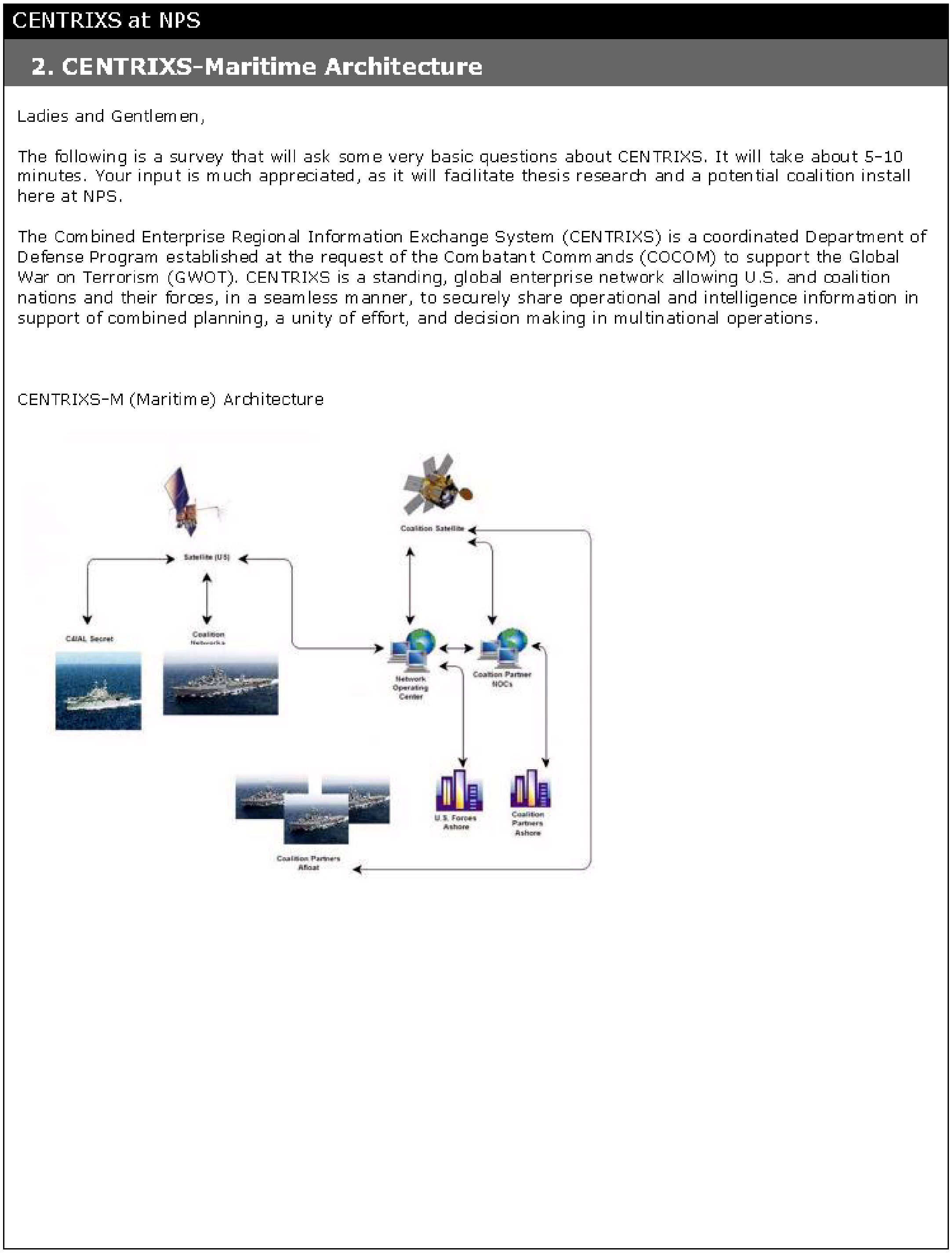
Voluntary Nature of the Survey. I understand that my participation is strictly voluntary, and if I agree to participate, I am free to withdraw at any time without prejudice.

Points of Contact. I understand that if I have any questions or comments regarding this project upon the completion of my participation, I should contact the Principal Investigator, LtCol Karl D. Pfeiffer, USAF, Asst. Professor, 831-656-3635, kdpfeiff@nps.edu. Any other questions or concerns may be addressed to the IRB Chair, LT Brent Olde, 656-3807, baolde@nps.edu.

Statement of Consent. I have been provided with a full explanation of the purpose, procedures, and duration of my participation in this survey. I understand how my identification will be safeguarded and have had all my questions answered. I have been provided a copy of this form for my records and I agree to participate in this survey. I understand that by agreeing to participate in this research, I do not waive any of my legal rights. By clicking the "Yes" button below, I agree to participate in the survey.

1. I agree to participate in the survey

○ Yes ○ No



CENTRIXS at NPS

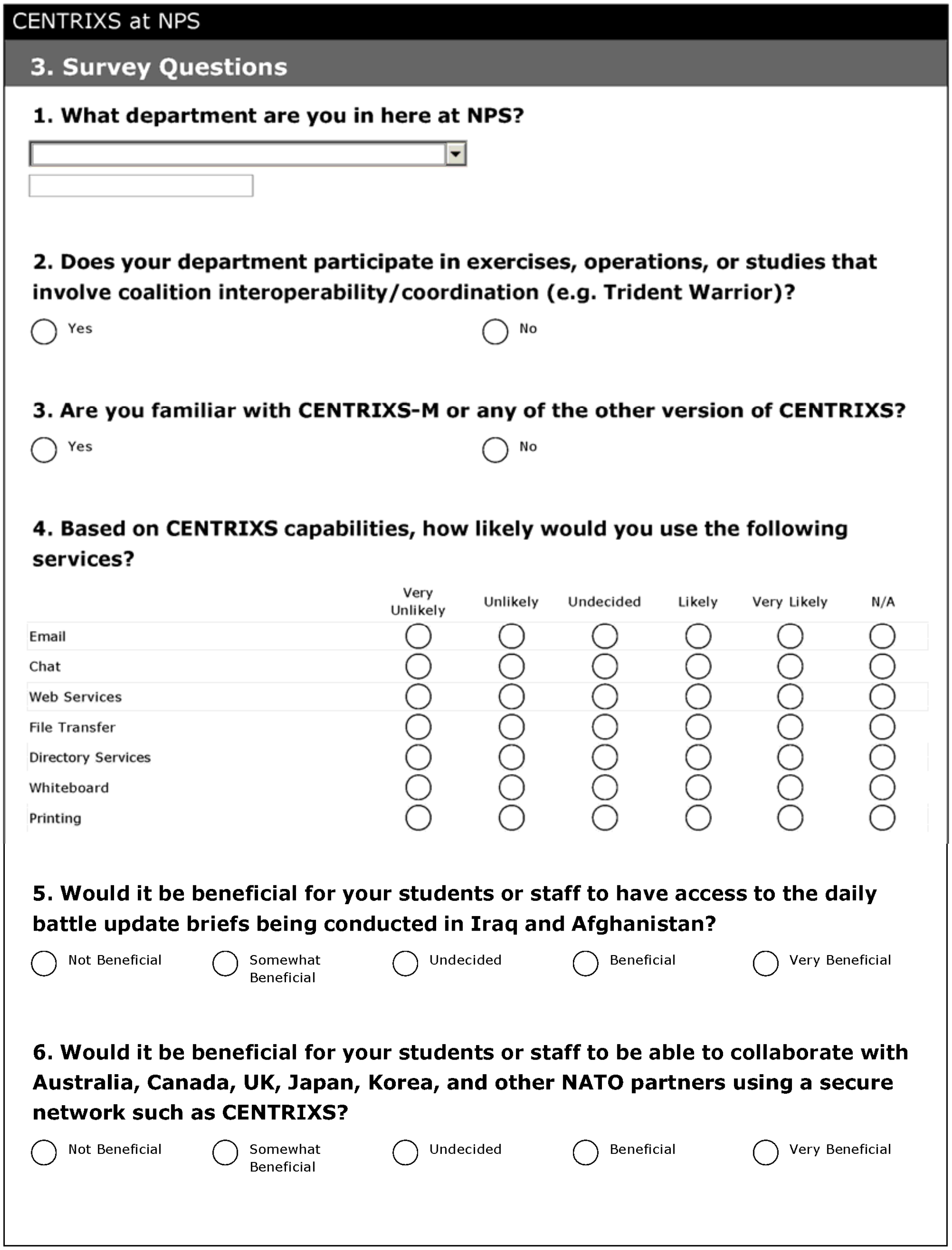
2. CENTRIXS-Maritime Architecture

Ladies and Gentlemen,

The following is a survey that will ask some very basic questions about CENTRIXS. It will take about 5-10 minutes. Your input is much appreciated, as it will facilitate thesis research and a potential coalition install here at NPS.

The Combined Enterprise Regional Information Exchange System (CENTRIXS) is a coordinated Department of Defense Program established at the request of the Combatant Commands (COCOM) to support the Global War on Terrorism (GWOT). CENTRIXS is a standing, global enterprise network allowing U.S. and coalition nations and their forces, in a seamless manner, to securely share operational and intelligence information in support of combined planning, a unity of effort, and decision making in multinational operations.

CENTRIXS-M (Maritime) Architecture



CENTRIXS at NPS

3. Survey Questions

1. What department are you in here at NPS?

2. Does your department participate in exercises, operations, or studies that involve coalition interoperability/coordination (e.g. Trident Warrior)?

○ Yes ○ No

3. Are you familiar with CENTRIXS-M or any of the other version of CENTRIXS?

○ Yes ○ No

4. Based on CENTRIXS capabilities, how likely would you use the following services?

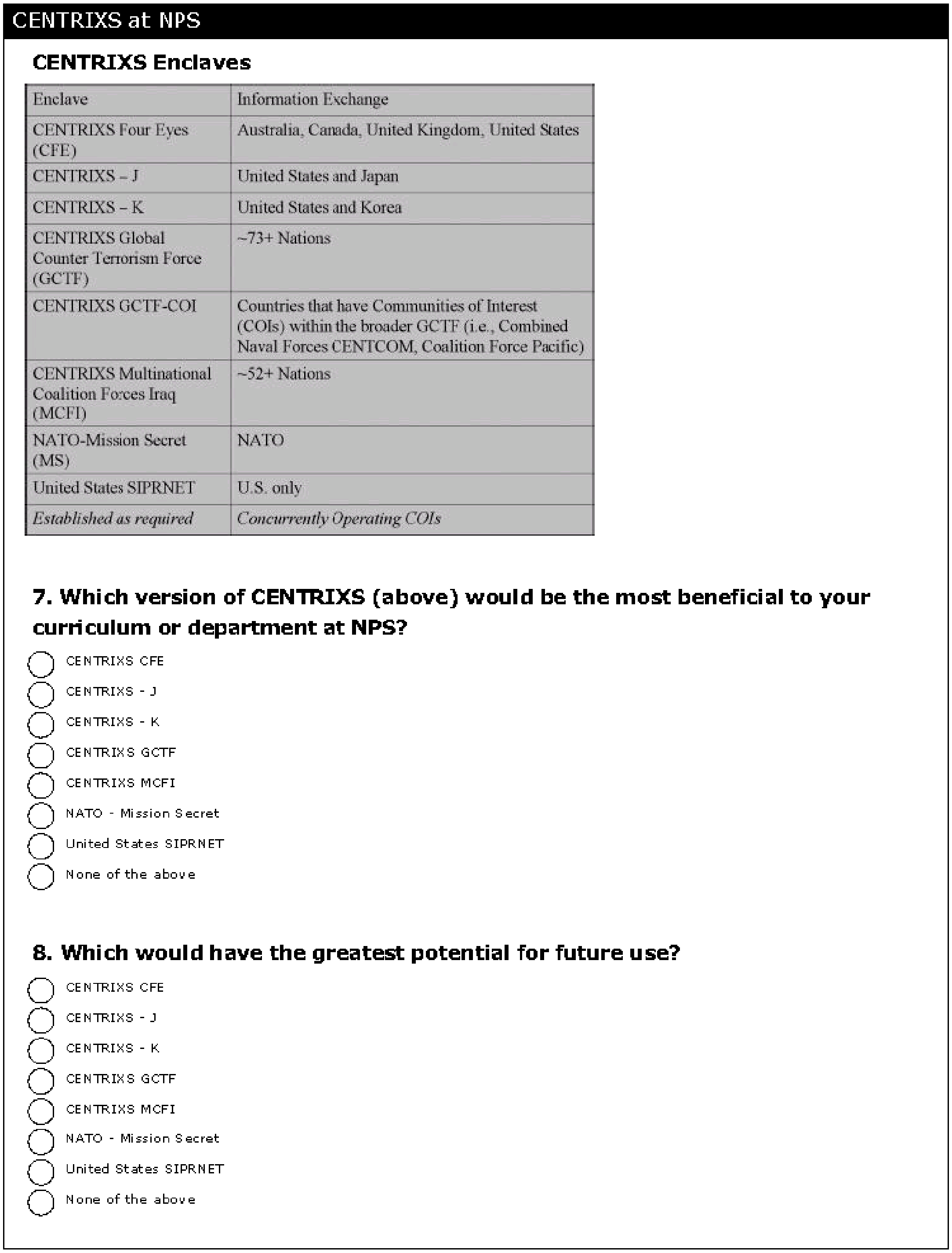
	Very Unlikely	Unlikely	Undecided	Likely	Very Likely	N/A
Email	○	○	○	○	○	○
Chat	○	○	○	○	○	○
Web Services	○	○	○	○	○	○
File Transfer	○	○	○	○	○	○
Directory Services	○	○	○	○	○	○
Whiteboard	○	○	○	○	○	○
Printing	○	○	○	○	○	○

5. Would it be beneficial for your students or staff to have access to the daily battle update briefs being conducted in Iraq and Afghanistan?

○ Not Beneficial ○ Somewhat Beneficial ○ Undecided ○ Beneficial ○ Very Beneficial

6. Would it be beneficial for your students or staff to be able to collaborate with Australia, Canada, UK, Japan, Korea, and other NATO partners using a secure network such as CENTRIXS?

○ Not Beneficial ○ Somewhat Beneficial ○ Undecided ○ Beneficial ○ Very Beneficial



CENTRIXS at NPS

CENTRIXS Enclaves

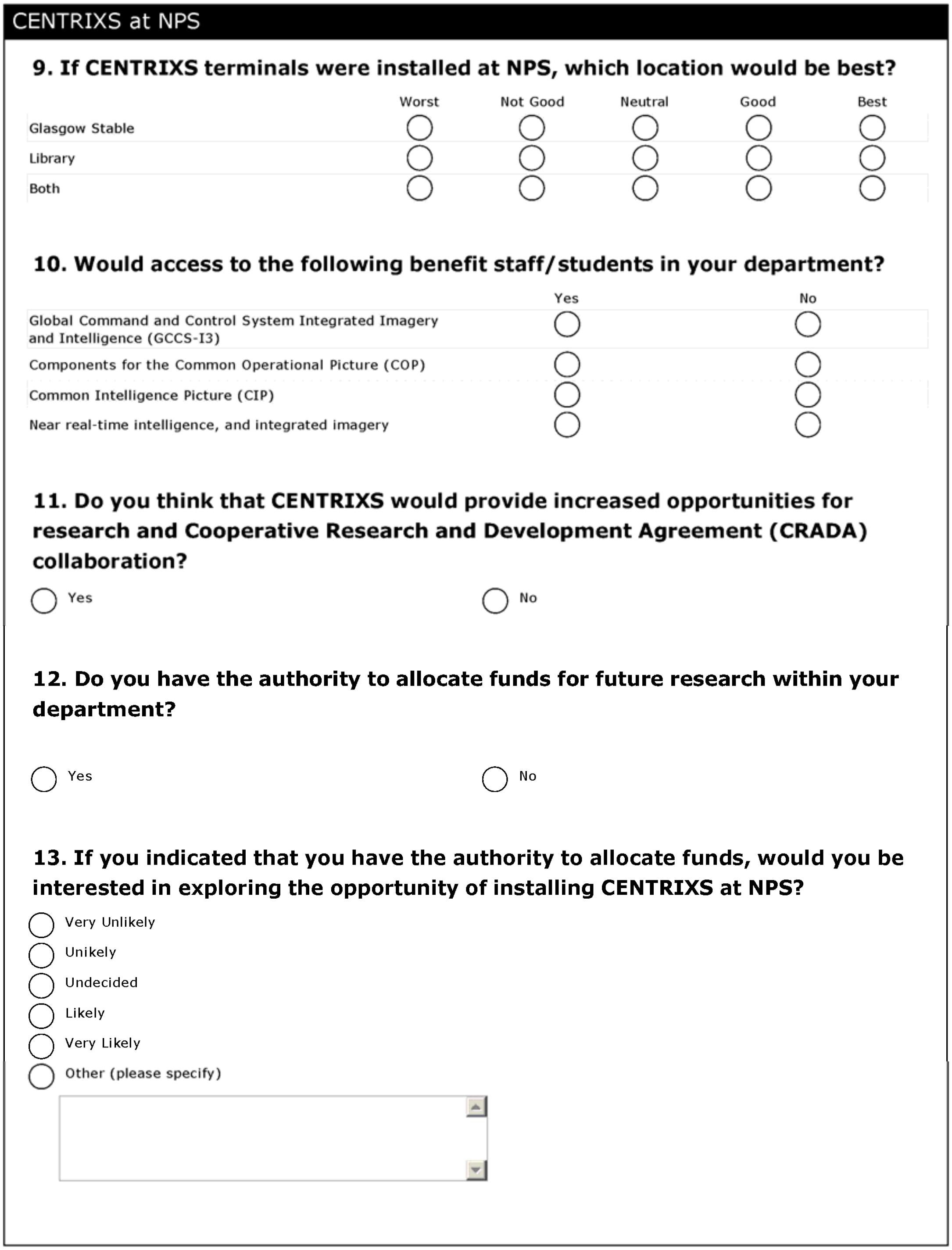
Enclave	Information Exchange
CENTRIXS Four Eyes (CFE)	Australia, Canada, United Kingdom, United States
CENTRIXS – J	United States and Japan
CENTRIXS – K	United States and Korea
CENTRIXS Global Counter Terrorism Force (GCTF)	~73+ Nations
CENTRIXS GCTF-COI	Countries that have Communities of Interest (COIs) within the broader GCTF (i.e., Combined Naval Forces CENTCOM, Coalition Force Pacific)
CENTRIXS Multinational Coalition Forces Iraq (MCFI)	~52+ Nations
NATO-Mission Secret (MS)	NATO
United States SIPRNET	U.S. only
Established as required	*Concurrently Operating COIs*

7. Which version of CENTRIXS (above) would be the most beneficial to your curriculum or department at NPS?

○ CENTRIXS CFE
○ CENTRIXS - J
○ CENTRIXS - K
○ CENTRIXS GCTF
○ CENTRIXS MCFI
○ NATO - Mission Secret
○ United States SIPRNET
○ None of the above

8. Which would have the greatest potential for future use?

○ CENTRIXS CFE
○ CENTRIXS - J
○ CENTRIXS - K
○ CENTRIXS GCTF
○ CENTRIXS MCFI
○ NATO - Mission Secret
○ United States SIPRNET
○ None of the above



CENTRIXS at NPS

9. If CENTRIXS terminals were installed at NPS, which location would be best?

	Worst	Not Good	Neutral	Good	Best
Glasgow Stable	○	○	○	○	○
Library	○	○	○	○	○
Both	○	○	○	○	○

10. Would access to the following benefit staff/students in your department?

	Yes	No
Global Command and Control System Integrated Imagery and Intelligence (GCCS-I3)	○	○
Components for the Common Operational Picture (COP)	○	○
Common Intelligence Picture (CIP)	○	○
Near real-time intelligence, and integrated imagery	○	○

11. Do you think that CENTRIXS would provide increased opportunities for research and Cooperative Research and Development Agreement (CRADA) collaboration?

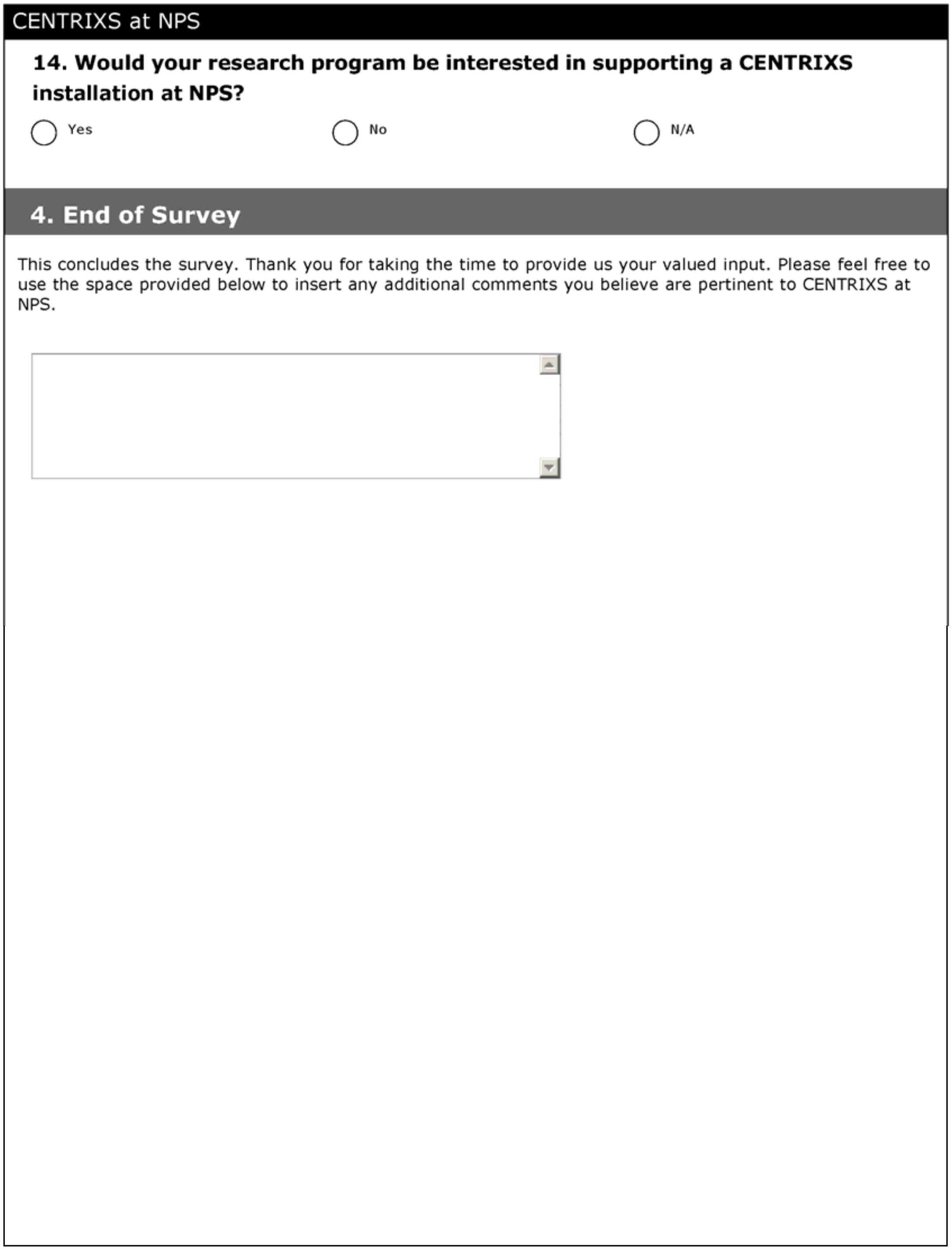
○ Yes ○ No

12. Do you have the authority to allocate funds for future research within your department?

○ Yes ○ No

13. If you indicated that you have the authority to allocate funds, would you be interested in exploring the opportunity of installing CENTRIXS at NPS?

○ Very Unlikely
○ Unikely
○ Undecided
○ Likely
○ Very Likely
○ Other (please specify)



CENTRIXS at NPS

14. Would your research program be interested in supporting a CENTRIXS installation at NPS?

○ Yes ○ No ○ N/A

4. End of Survey

This concludes the survey. Thank you for taking the time to provide us your valued input. Please feel free to use the space provided below to insert any additional comments you believe are pertinent to CENTRIXS at NPS.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Bayer, Virginia. SPAWAR PMW-160 PRNOC CENTRIXS Engineer. Phone conversation April 2007.

Boardman, J., & Shuey, D. "Combined Enterprise Regional Information Exchange System (CENTRIXS); Supporting Coalition Warfare World-Wide." USCENTCOM. 2004.

Brewin, Bob. *Federal Computer Weekly*, "DISA in, Navy out on CENTRIXS," Article 97622, 12 February 2007.

Ching, Kenneth. SPAWAR PMW-160 PRNOC CENTRIXS Engineer. Phone conversation April 2007.

CJCSINST 6285.01, 1 August 2006.

CJCS J6 Joint Communication Systems Campaign Plan, Trident Warrior 2006, July 2006.

CJSINST 3170.01F, February 2007.

Clements, P., Kazman R. & Klein, M. "Evaluating Software Architecture: Methods and Case Studies." Addison Wesley, 2002.

Cochrane, C.D., Defense Acquisition University Press, "Introduction to Defense Acquisition Management" Sixth Edition, 2003.

Cochrane, C. D., Defense Acquisition University Press, "Program Managers Tool Kit," 14th Edition, 2005.

Department of the Navy Fiscal Year (FY) Fiscal Year 2008/2009 Budget Estimates, February 2007.

Department of the Navy PEO C4I, Canes Roadmap, PMW-160, November 2006.

Department of the Navy PEO C4I, Information Assurance and Enterprise Services, 2006.

DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD (C3I))." 1992.

DoD Information Assurance, Certification and Accreditation Process (DIACAP), 6 July 2006.

DoD Instruction 8110.1. "Multinational Information Sharing Networks Implementation." February 2004.

DoD PEO C4I, Networks, Information Assurance and Enterprise Services (PMW160), 7 November 2006.

Fetter, Delores, Naval Acquisition Enterprise Panel, “Building the Naval Acquisition Enterprise,” Slide 36, 2006.

Integrated Defense Acquisition, Technology, and Logistics (IDATL), Life Cycle Management Framework, DAU Press, 2005.

Joint Chiefs of Staff (JCS), “Joint Communication Systems Campaign Plan, Trident Warrior 2006,” July 2006.

Joint Interoperability Test Command (JITC) home page, http://jitc.fhu.disa.mil/washops/jtca/centrixs.html, Last Accessed June 2007.

McGufrie, Michael., SPAWAR Allied Coalition Framework Brief, 2003.

Military Communications Electronics Board (MCEB) Pub 1, 1 March 2002.

MIP 4952/008, Navy Preventive Maintenance System, 2007.

NDP-1. “National Disclosure Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations.” 2002.

PMW-160 Financial Management and Cost Estimating Support, Performance Work Statement (PWS), 20 June 2006.

Preventive Maintenance System, Maintenance Index Page (MIP) 4952/008.

SECNAVINST 5000.2C, Table E2T1 Joint Interoperability Test Command (JITC), “CENTRIXS” Web site home page.

Secret and Below Interoperability (SABI) Process Panel, NIST Conference Abstract, 1998.

Shannon, Joseph. SPAWAR PMW-160 Engineer. Phone conversation May 2007.

Soriano, PMW 160.1, AFCEA Symposium Brief, 23 May 2007.

Soriano, PMW 160.1, Armed Forces Communications and Electronics Association (AFCEA) C4I Symposium Brief, 2007.

SPAWAR Master Series web site, www.teammantech.com/masterseries/main/vforums/centrixs/vforum.swf, Last Accessed June 2007.

United States Central Command (USCENTCOM). CENTRIXS CONOPS for Multinational Operations. December 2004.

United States Central Command (USCENTCOM). Theater Security Cooperation Strategy. March 2003.

United States Navy website, http://www.navy.mil/search/display.asp?story_id=30603, Last Accessed August 2007.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Fort Belvoir, Virginia

2. Dudley Knox Library
Naval Postgraduate School
Monterey, California

3. Marine Corps Representative
Naval Postgraduate School
Monterey, California

4. Director, Training and Education, MCCDC, Code C46
Quantico, Virginia

5. Director, Marine Corps Research Center, MCCDC, Code C40RC
Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
Camp Pendleton, California